4/2013

Datenschutz Nachrichten

36. Jahrgang
ISSN 0137-7767
9,00 Euro



■ Europäisches Datenschutzrecht ist notwendiger denn je! ■ Europa muss den Datenschutz retten! ■ Eine Datenschutzgesetzgebung für das 21. Jahrhundert ■ Die richtige Balance im Datenschutzrecht ■ Fortschritte in hitzigen Zeiten ■ Gut für den Beschäftigtendatenschutz? ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechung ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine

Montag, 27. Januar 2014, 18:00 Uhr
Wie sicher sind unsere Daten?
Wie können wir uns schützen?
Technologische Aspekte der Internetüberwachung und der Kryptographie
Berlin-Grunewald, Bismarckallee 46/48
Einführung: Peter Schaar (Vorsitzender der EAID)
Vorträge: Prof. Dr. Hannes Federrath (Universität Hamburg, Fachbereich Informatik), Michael Hange (Präsident des Bundesamts für die Sicherheit in der Informationstechnik)
Constanze Kurz (Sprecherin des Chaos Computer Clubs)
Diskussionsleitung: (Dr. Alexander Dix, Berliner Beauftragter für Datenschutz und Informationsfreiheit)

Samstag, 01. Februar 2014
Redaktionsschluss DANA 1/2014
Thema: Konzerndatenschutz
Verantwortlich: Karin Schuler

Samstag, 22. Februar 2014, 10:00-14:00 Uhr
DVD-Vorstandssitzung
Bonn. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Freitag, 11. April 2014, 18:00 Uhr
BigBrotherAwards
Verleihung der Negativ-Preise für Datenkraken
Bielefeld, Hechelei

Samstag, 12. April 2014, 09:30 Uhr
DVD-Vorstandssitzung
Bielefeld. Anmeldung in Geschäftsstelle
dvd@datenschutzverein.de

Donnerstag, 01. Mai 2014
Redaktionsschluss DANA 2/2014
Thema: Internet der Dinge
Verantwortlich: NN

DANA
Datenschutz Nachrichten
ISSN 0137-7767
36. Jahrgang, Heft 4

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftstelle:
Rheingasse 8-10, 53113 Bonn
Tel. 0228-222498
Konto 1900 2187, BLZ 370 501 98, Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Karsten Neumann
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Rheingasse 8-10, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@t-online.de

Druck
Onlineprinters GmbH
Rudolf-Diesel-Straße 10
91413 Neustadt a. d. Aisch
www.diedruckerei.de
Tel. +49 (0)91 61 / 6 20 98 00
Fax +49 (0) 91 61 / 66 29 20

Bezugspreis
Einzelheft 9 Euro. Jahresabonnement 32 Euro (incl. Porto) für vier Hefte im Jahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen, Fotos
Frans Jozef Valenta, soweit nicht anders gekennzeichnet

Editorial

Liebe Leserinnen, liebe Leser,

NSA und britischer Geheimdienst haben den Albtraum lebendig gemacht, vor dem das Bundesverfassungsgericht im Volkszählungsurteil warnte: eine solche Gesellschaftsordnung wäre weder demokratisch noch frei – so das Fazit einer detaillierten und informativen Analyse des englischen Rechtsprofessors Douwe Korff. Ein starkes europäisches Datenschutzrecht ist die berechtigte Erwartung der internationalen Öffentlichkeit an Europaparlament und die europäischen Regierungen. 30 Jahre nach der Volkszählungsentscheidung und nach 12 Jahren Kampf gegen den Terror stehen wir vor einer Zäsur – in unserem rechtsstaatlichen Selbstverständnis als demokratisches Gemeinwesen. Einfacher geht es nicht – die Beiträge dieses Heftes belegen es eindrücklich und vielstimmig.

Karsten Neumann

Autorinnen und Autoren dieser Ausgabe:

Jan Philipp Albrecht
Innen- und justizpolitischer Sprecher der Grünen im Europäischen Parlament sowie Berichterstatter des Europäischen Parlaments für die neue EU-Datenschutzverordnung, jan.albrecht@europarl.europa.eu

Alexander Alvaro
Innenpolitischer Sprecher der FDP im Europäischen Parlament,
alexander.alvaro@europarl.europa.eu

Cornelia Ernst
Innen- und justizpolitischer Sprecherin für DIE LINKE im Europäischen Parlament,
cornelia.ernst@europarl.europa.eu

Peter Hustinx
Europäischer Datenschutzbeauftragter, peter.hustinx@edps.europa.eu

Douwe Korff
Professor für Internationales Recht an der London Metropolitan Universität,
d.korff@londonmet.ac.uk

Peter Schaar
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI),
eu-datenschutz@bdfi.bund.de

Birgit Sippel
SPD-Europaabgeordnete für Südwestfalen. Mitglied im Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres (LIBE). Stellv. Mitglied im Ausschuss für Beschäftigung und soziale Angelegenheiten (EMPL) birgit.sippel@europarl.europa.eu

Axel Voss
Mitglied des Europäischen Parlaments für die Region Mittelrhein.
axel.voss@europarl.europa.eu

Peter Wedde
Direktor der Europäischen Akademie der Arbeit in der Universität Frankfurt am Main
Professor für Arbeitsrecht und Recht der Informationsgesellschaft.
AdA@em.uni-frankfurt.de



Peter Schaar

PRISM, Tempora & Co.: Ein starkes Europäisches Datenschutzrecht ist notwendiger denn je!

Eigentlich hätte es keines Beweises mehr bedurft, aber die Enthüllungen des ehemaligen Mitarbeiters des US-Geheimdienstes NSA haben nun auch vielen Skeptikern deutlich gemacht, dass unsere Daten keineswegs so sicher sind, wie vielfach suggeriert wird.

Wie sieht die Situation derzeit aus? Einige wenige, meist nicht in Europa ansässige Unternehmen beherrschen weitgehend die Märkte für die relevanten Massenanwendungen im Bereich von Information und Kommunikation. Die amerikanischen Marktführer für Suchmaschinen oder soziale Netzwerke, und zwei bis drei Anbieter von Betriebssystemen für mobile Endgeräte wie Smartphones oder Tablets haben monopolartige Strukturen aufgebaut. Diese Unternehmen sammeln unvorstellbare Datenmengen, die einen erheblichen Machtfaktor darstellen – ein Problem nicht nur für die Privatsphäre der Nutzerinnen und Nutzer. Die Möglichkeiten der Verknüpfung und Auswertung im Rahmen von „Big Data" und die Auslagerung großer Datenmengen in weltweite Clouds verdeutlichen die Dimension der Risiken für den Umgang mit vertraulichen Dokumenten mit oder ohne Personenbezug. Wie bedenklich diese Entwicklung ist, wird nun besonders deutlich, wenn man sieht, dass die großen IT-Unternehmen – teils auf „offiziellem" Wege, teils unwissentlich – Zugriffen durch Geheimdienste ausgesetzt sind. Besonders bedenklich stimmen Berichte über eine enge (überobligatorische) Zusammenarbeit zwischen Geheimdiensten und Internetdiensten.

Wie Umfragen zeigen, sind die Menschen durchaus besorgt: Sie halten ihre Privatsphäre für einen wichtigen Wert. Das Vertrauen in den Schutz der Daten und die Sicherheit der Informations- und Kommunikationstechnologie ist stark beschädigt. Gleichzeitig ist fast jeder auf die Nutzung dieser Technologien angewiesen und so droht sich eine Art Fatalismus auszubreiten, dass man gegen den Verlust der Privatsphäre letztlich machtlos sei – eine für eine demokratische Gesellschaft gefährliche Entwicklung.

Kann die europäische Datenschutzreform einen Beitrag dazu leisten, dass das Machtgefälle zwischen Datenverarbeitern und Nutzern verringert und das Vertrauen in den Schutz der Privatsphäre wieder gestärkt wird? Ich denke ja. Natürlich kann das europäische Datenschutzrecht allein nicht die Zugriffe von Geheimdiensten verhindern. Dies ist schon deshalb nicht möglich, weil sich weder der Anwendungsbereich der Datenschutz-Grundverordnung (DSGVO) noch der Richtlinie für den Polizei- und Justizbereich (JI-Richtlinie) auf die Datenverarbeitung von Geheimdiensten erstreckt. Hier bedarf es internationaler Vereinbarungen und einer rechtsstaatlichen und transparenten Kontrolle der Geheimdienste. Zudem muss die technologische Sicherung des Datenschutzes – z. B. durch wirksame Verschlüsselungsverfahren – gefördert und verbreitet werden.

Dennoch kann die europäische Datenschutzreform die Situation verbessern. Ein besonders wichtiger Gesichtspunkt ist dabei die Einführung des so genannten Marktortprinzips in Art. 3 Abs. 2 DSGVO. Unternehmen, die Waren oder Dienstleistungen in Europa anbieten oder deren Datenverarbeitung der Beobachtung Betroffener in der EU dient, sollen auch dann dem europäischen Datenschutzrecht unterliegen, wenn sie keinerlei Niederlassung innerhalb der EU haben. Damit werden ein einheitliches Datenschutzniveau und gleiche Wettbewerbsbedingungen für alle Unternehmen hergestellt, die den europäischen Markt adressieren.

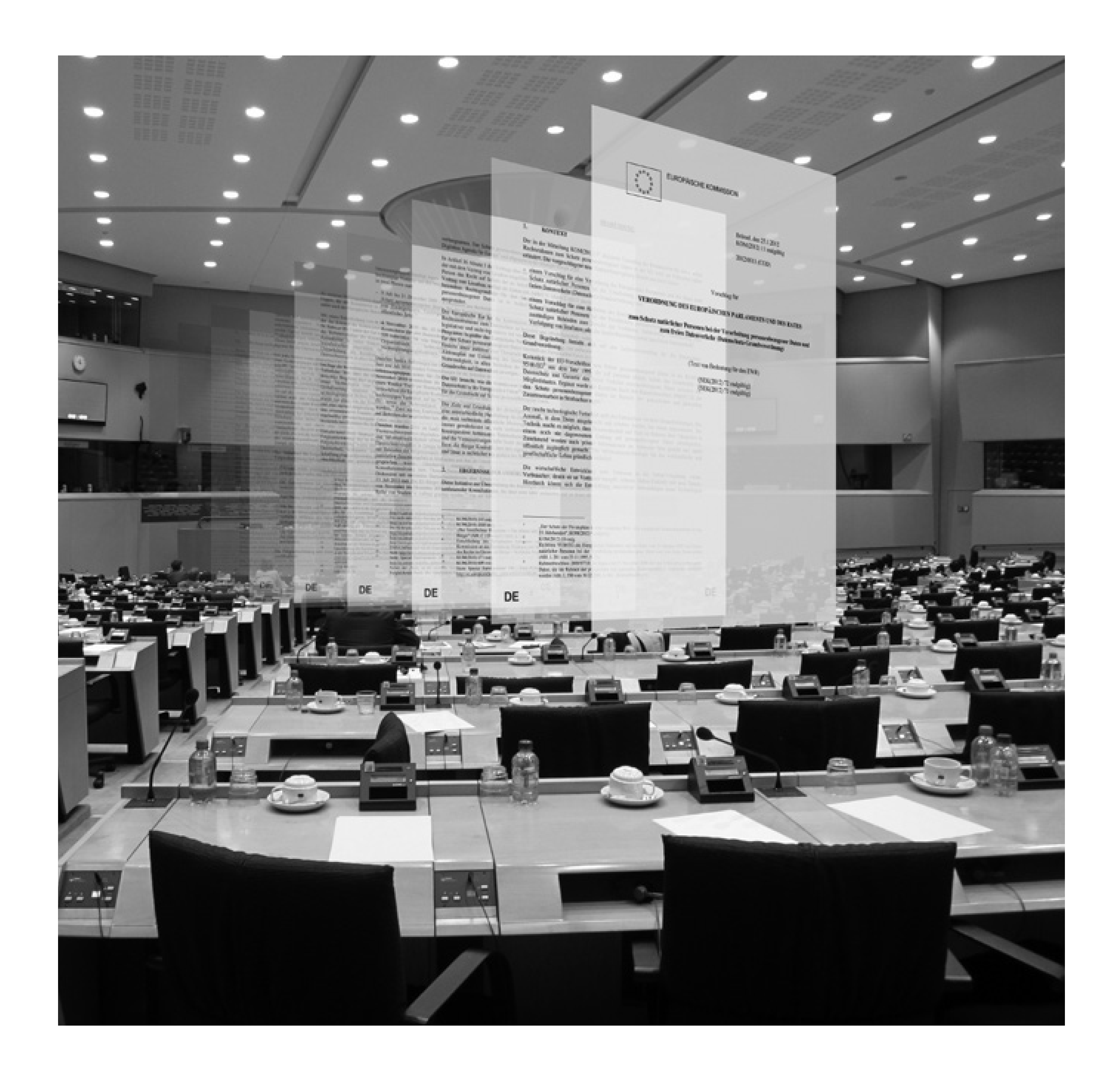
Der Entwurf der DSGVO enthält darüber hinaus eine Reihe weiterer Elemente zur Stärkung des Datenschutzes, wie z. B. bei der Stärkung der Einwilligung, der Begrenzung der Profilbildung, der Verbesserung des technologischen Datenschutzes oder der Einführung wirksamer Sanktionen.

Die nunmehr vom Europäischen Parlament (EP) am 21. Oktober 2013 vorgelegten Vorschläge zum Entwurf der DSGVO sind außerordentlich positiv zu bewerten und heben sich sehr von den mühsamen Verhandlungen im Rat der EU ab. Die vom LIBE-Ausschuss vorgeschlagene Stärkung der Einwilligung, die Einführung icon-basierter Datenschutzinformationen, die weitere Begrenzung der Profilbildung oder das klare Bekenntnis zur Bestellung betrieblicher Datenschutzbeauftragter sind nur einige Beispiele, die den Datenschutz stärken und damit für mehr Augenhöhe zwischen Datenverarbeitern und dem Einzelnen sorgen können.

Angesichts der aktuellen Ereignisse ist vor allem aber auch auf den vom LIBE-Ausschuss vorgeschlagenen Art. 43a DSGVO hinzuweisen. Nach dieser Vorschrift sollen Datenübermittlungen an ausländische Behörden und Gerichte nur noch auf der Basis von Rechtshilfeabkommen oder internationalen Vereinbarungen erlaubt sein. Zudem sollen die Aufsichtsbehörden und die Betroffenen über solche Zugriffe informiert werden. Darüber hinaus besteht für die Datenübermittlungen ein Genehmigungsvorbehalt durch die Aufsichtsbehörden. Dies wird Zugriffe z. B. von ausländischen Geheimdiensten nicht verhindern. Es kann aber zu einem großen Teil sichergestellt werden, dass personenbezogene Daten von Europäerinnen und Europäern nur nach

den Maßstäben des europäischen Rechts und mit einer weitgehenden Transparenz für den Einzelnen weitergegeben werden dürfen. Dabei ist zu berücksichtigen, dass diese Regeln aufgrund des Marktortprinzips auch für außereuropäische Unternehmen gelten. Wir sollten an diesem Punkt aber nicht stehen bleiben: Auch die Zugriffe durch europäische Geheimdienste gehören auf den Prüfstand und müssen vergleichbaren Anforderungen unterliegen – das europäische Grundrecht auf Datenschutz ist nicht teilbar und gilt gegenüber ausländischen wie inländischen Stellen.

Zwar gilt in der EU – anders als Deutschland – keine strenge Diskontinuitätsregel, nach der alle in einer Legislaturperiode nicht abgeschlossenen Vorhaben neu begonnen werden müssen. Trotzdem ist es alles andere als sicher, dass ein neu zusammengesetztes EP und eine veränderte Europäische Kommission bei den bisherigen Ergebnissen weitermachen werden. Ich halte es für nicht ausgeschlossen, dass die Datenschutzreform auch in den kommenden fünf Jahren nicht gelingen wird, wenn die Verhandlungen im EU-Rat, die Vertretung der Regierungen der Mitgliedstaaten, nicht zu einem zügigen Ende kommen – mit der Konsequenz der weiteren Erosion des Datenschutzes in Europa. Deshalb hoffe ich, dass auch der Rat die Zeichen der Zeit erkennt und – gemeinsam mit dem Parlament und der Kommission – für eine zügige Verabschiedung eines starken harmonisierten europäischen Datenschutzrechts noch vor den Wahlen zum Europäischen Parlament sorgt.





Jan Philipp Albrecht

Europa muss den Datenschutz retten!

Die Massenüberwachungsprogramme des US-amerikanischen Geheimdienstes NSA und des britischen Geheimdienstes GCHQ haben die Welt schokkiert. Mittels elektronischer Ausspähung von Telefonaten, E-Mails und Surfverhalten können diese Dienste von uns allen ein Profil unserer Persönlichkeit anlegen und unser ganzes Leben ausforschen. Es ist vollkommen klar: Geheimdienste haben schon immer spioniert und sie werden es wohl auch weiterhin tun. Aber ist es wirklich richtig, dass dabei keine Grenzen mehr gelten? Ist es richtig, dass große Internetkonzerne wie Google, Yahoo und Facebook uns allen vermitteln, unsere Daten wären bei ihnen sicher, wenn dies gar nicht so ist? Nein, es muss endlich aufhören mit der Naivität beim Datenschutz. Für unsere personenbezogenen Daten braucht es scharfe gesetzliche Regeln wie im Straßenverkehr und im Strafrecht. Wer andere ausspäht, ohne dass dafür deren explizite Zustimmung oder eine verhältnismäßige Gesetzesgrundlage vorliegt, muss mit deftigen Strafen rechnen. Nichts anderes haben EU-Kommission und Europäisches Parlament mit der EU-Datenschutzverordnung vorgeschlagen. Sie würde die Kontroll- und Selbstbestimmungsrechte für die einzelnen Menschen verbessern und den Datenschutzbehörden der EU klare Regeln zur Verfolgung von Rechtsverletzungen in der ganzen EU an die Hand geben. Auch gegenüber Akteuren von außerhalb. Es wäre dringend nötig, dass die Regierungen der EU diese vor der Europawahl im Mai 2014 verabschieden.

Zudem muss klar sein: Wenn Staaten Regeln brechen – so wie es die USA und Großbritannien offenbar tun – kann so etwas nicht ohne Konsequenzen bleiben. Der Einbruch in Telekommunikationssysteme und Unternehmen muss umgehend von höchster Ebene verurteilt und von Ermittlern verfolgt werden. Ansonsten wird das Vertrauen in Demokratie und Rechtsstaat erheblichen Schaden nehmen. In der Untersuchung des Europäischen Parlaments zu den Enthüllungen von Edward Snowden wurde allerdings klar: Noch hat keine Ermittlungsbehörde der EU-Staaten das neue Cybercrime-Center von Europol (EC3) um Hilfe bei der Ermittlung von Angriffen wie jenen auf das belgische Unternehmen Belgacom oder die Server von Google und Yahoo in Finnland gebeten. Wenn Europa sein Recht nicht nur auf dem Papier, sondern auch in der Praxis durchgesetzt haben will, dann müssen jetzt Konsequenzen folgen. Im Falle Großbritanniens wäre es daher angebracht, ein Vertragsverletzungsverfahren einzuleiten, um die Unterwanderung des EU-Rechts durch den GCHQ endgültig zu beenden. Bei den USA muss Europa vor allem diplomatischen Druck ausüben. Die Aussetzung von Datenaustauschabkommen wie SWIFT und Safe Harbour wäre konsequent, wenn die Datenschutzrechte von EU-Bürgern bedroht sind. Auch die Verhandlungen zum Freihandelsabkommen zwischen EU und USA sollten erst dann weitergeführt werden, wenn die USA ihre Massenüberwachung beenden.

Für die einzelnen Bürgerinnen und Bürger ist es nun an wichtig, endlich Druck auf die Parteien auszuüben. Jede Partei, die die Zeichen der Zeit nicht erkannt hat, muss für Untätigkeit und mangelnde Konsequenz abgestraft werden. Gleiches gilt für den wirtschaftlichen Druck durch Verbraucherinnen und Verbraucher: Die Nutzung von kompromittierten Diensten sollte umgehend eingestellt werden. Stattdessen müssen wir jetzt nach Diensten und Produkten suchen, die Datenschutz als wichtigstes und verlässliches Merkmal enthalten. Dabei geht es nicht nur um Verschlüsselung und Systemsicherheit, sondern auch um die technischen Vorrichtungen, die Kontrolle über die eigenen personenbezogenen Daten erlauben. Dazu gehören hemmungslose Transparenz für die Nutzerinnen und Nutzer sowie ein Fokus auf die Minimierung von personenbezogenen Daten. Unternehmen müssen endlich einen Wettlauf starten, wer die besten Dienste unter Einbeziehung der wenigsten Nutzerdaten anbietet. Über Jahre hinweg haben viele große Internetkonzerne uns weismachen wollen, dass Datenschutz einfach kein Wettbewerbsvorteil, sondern ein großer Kostenfaktor sei. Durch die Ereignissen der letzten Monate gibt es die Möglichkeit, ihnen endlich das Gegenteil zu beweisen und gemeinsam mit zukunfts- und werteorientierten Unternehmen für die Rettung des Datenschutzes in der digitalen Welt zu kämpfen.

Es ist allerhöchste Zeit. Denn viel zu lange hat die Politik den Datenschutz als rein technische Materie und das Internet als national regierbaren Raum betrachtet. Beides waren große Irrtümer, die uns eine entfesselte Überwachungsgesellschaft geliefert haben. Es ist jetzt an der Zeit, die Auswüchse dieser Entwicklung wieder zu beseitigen. Auch wenn einige schon mit den Dollarzeichen in den Augen von der großen Ausbeutung der persönlichen Informationen geträumt haben – es ist unsere Aufgabe, sie wieder auf den Boden der Tatsachen einer demokratischen, wertebasierten Gesellschaft zurückzuholen.



Alexander Alvaro

Eine Datenschutzgesetzgebung für das 21. Jahrhundert

Die aktuell geltende europäische Datenschutzgesetzgebung ist siebzehn Jahre alt und in einer Zeit verfasst worden, als es weder eCommerce noch soziale Netzwerke gab und Flugtickets noch nicht online gebucht wurden.

Verbraucher haben sich mittlerweile an die Vorteile, die die moderne Informations- und Kommunikationstechnologie geschaffen hat, gewöhnt. Personenbezogene Daten sind in der Folge zu einer “Währung” für alltäglich gewordene Dienstleistungen geworden. Zentral bleibt aber, dass die letztliche Verfügungsgewalt beim Nutzer bleiben muss. Es müssen also durchsetzbare Standards geschaffen werden. Nur so kann die nötige Balance zwischen den Grundrechten und der Entwicklung innovativer, digitaler Geschäftsmodelle geschaffen werden.

Im Oktober 2013 verabschiedete das Europäische Parlament nach monatelanger Beratung einen Vorschlag für eine neue Datenschutzverordnung, die in ihrer aktuellen Fassung das Potenzial hat, einen Datenschutz zu schaffen, der den Erfordernissen des 21. Jahrhunderts gerecht wird.

Die Liberalen haben sich dafür eingesetzt, dass all diejenigen, die Daten verarbeiten, in Zukunft in ein nachhaltiges Datenmanagementsystem investieren und dafür Sorge tragen müssen, dass die durch dieses System festgelegten Schutzmechanismen auch durchgängig eingehalten werden. Die Eckpunkte eines solchen Systems wurden 2012 unter dem Titel “Lifecycle Data Protection Management” von der FDP im EP vorgelegt und sind in den Vorschlag eingeflossen. Acht Eckpunkte sind zentral:

1. Datenschutz durch Design: Eine wichtige Grundvoraussetzung für den nachhaltigen Schutz personenbezogener Daten ist der systematische Einsatz von „Datenschutz durch Design“. Dies bedeutet, dass systematisch Schutzvorkehrungen zum Einsatz kommen müssen, die neben der Richtigkeit, Vertraulichkeit und der Integrität auch die physische Sicherheit personenbezogener Daten gewährleisten.
2. Datenschutzfreundliche Voreinstellungen: Nur Daten, deren Verarbeitung für den jeweiligen spezifischen Zweck auch unbedingt erforderlich ist, sollen verarbeitet werden dürfen. Zusätzlich sollten datenschutzfördernde Technologien, wie Verschlüsselungs- oder Anonymisierungsverfahren, abhängig vom Kontext und den jeweiligen Risiken der Datenverarbeitung, verpflichtend eingesetzt werden.
3. Folgenabschätzungen der Datenverarbeitung: Zentral ist hier eine Risikoanalyse, die versucht zu entdecken, ob eventuell Schwachstellen bestehen. Sicherlich können sie unter Umständen einen Mehraufwand für Unternehmen bedeuten, sie garantieren jedoch, dass Firmen sich von Beginn an der Konsequenzen ihrer Datenverarbeitungsvorgänge bewusst werden.
4. Regelmäßige Compliance Reviews: Datenverarbeiter sollten regelmäßige Überprüfungen durchführen. Sie dienen in erster Linie der Kontrolle der eingesetzten Datenschutzmaßnahmen und der gemachten Zusicherungen und sollten vom Kontext und den konkreten Risiken, die die Datenverarbeitungsvorgänge bergen, abhängen.
5. Faire und vergleichbare Informationspolitik: Nutzern ist häufig nicht bewusst, zu welchen Konditionen sie Daten preisgeben, um Internetdienste nutzen zu können. Sinnvoll wäre deshalb die Einführung iconbasierter Datenschutzerklärungen (ähnlich wie Verkehrszeichen). Diese sollten aus drei Spalten bestehen: Icon, wichtige Informationen, und eine Spalte in der angegeben ist, ob die Kriterien erfüllt sind oder nicht.
6. Schadensbasierte Risikoschwellen: Neben dem Kontext müssen auch die potenziellen Risiken eines Schadens bzw. eines Datenschutzvergehens im Zuge der Datenverarbeitung berücksichtigt werden; Parameter sind unter anderem die Anzahl der betroffenen Personen, deren Daten verarbeitet werden sowie die Sensibilität der bereitgestellten Daten.
7. Anreizgebende Sanktionsmaßnahmen: Diese sollten nicht primär bestrafen, sondern anreizgebend gestaltet sein, so dass Verstöße und Verletzungen von vornherein vermieden werden bzw. nicht wiederholt werden. Eine mögliche Sanktion könnte auch, anstelle von Geldbußen, die Auferlegung regelmäßiger Audits der für die Verarbeitung Verantwortlichen bedeuten.
8. Eine Datenschutzgesetzgebung für das 21. Jahrhundert sollte also darauf achten, dass die richtige Balance zwischen der Achtung der Grundrechte und der Entwicklung innovativer Geschäftsmodelle im digitalen Bereich eingehalten wird. Dabei darf aber nicht über das Ziel hinausgeschossen werden. Ein Bäckermeister legt Daten aus anderen Gründen an als ein Anbieter sozialer Netzwerke. Die Kosten für kleine und mittelständische Betriebe müssen deshalb in überschaubaren Grenzen bleiben.



Cornelia Ernst

Ein guter Kompromiss...

Nach monatelangen Verhandlungen unter uns Abgeordneten, die sich die meiste Zeit als sehr zäh erwiesen, konnte am 21. Oktober endlich im Innenausschuss abgestimmt werden. Auch DIE LINKE hat bei dieser Gelegenheit für den Kompromiss gestimmt. Insgesamt, finde ich, ist hier eine Einigung erreicht worden, die sich durchaus sehen lassen kann.

Die Vorzüge des beschlossenen Textes sind nicht wenige, sie darzustellen will ich aber an dieser Stelle anderen überlassen. Stattdessen möchte ich mich auf die aus meiner Sicht wichtigsten Punkte beschränken, die wir im Rahmen des gesamten Kompromisses akzeptieren konnten, die aber, für sich genommen, meine Zustimmung nicht gefunden hätten. Bei der Abstimmung wurden die meisten Artikel auf einen Schlag als Block beschlossen. Ich hatte beantragt, zwei dieser Artikel aus dem Block herauszunehmen und einzelnen abzustimmen. Dabei handelte es sich um die Artikel 6 und 20, denen ich die Zustimmung verweigert habe.

Auszug aus Artikel 6
Rechtmäßigkeit der Verarbeitung

f) Die Verarbeitung ist zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Dieser gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

Der Artikel 6 ist natürlich eines der zentralen Stücke der Verordnung. Die dort niedergelegten Kriterien für die Rechtmäßigkeit von Datenverarbeitung sind das A und O eines vernünftigen Datenschutzregimes. Die meisten Probleme verursacht die Datenverarbeitung auf Grundlage des sogenannten berechtigten Interesses. Diese Grundlage vollständig und ersatzlos zu streichen erschien jedoch nicht zweckmäßig, daher habe ich mich für eine deutliche Einschränkung stark gemacht. Ziel war es, die Verarbeitung aufgrund des berechtigten Interesses von Dritten, denen die Daten zur Verfügung gestellt wurden, zu verbieten. In jedem Fall kollidiert die Verarbeitung aufgrund berechtigter Interessen mit dem Grundprinzip der Zweckbindung. Kommt noch eine Weitergabe an Dritte hinzu, ist die Kontrolle über die Daten für die Menschen kaum noch auszuüben.

Das gleiche gilt für das Thema „Profiling". In der Verordnung wird das in Artikel 20 geregelt werden und auch da war ich nicht zufrieden mit dem Kompromiss. Zu Profiling sind in den Kompromissen insgesamt einige Verbesserungen zu finden, so ist der Anwendungsbereich von Artikel 20 deutlich erweitert worden. Die Logik, auf der eine Profilbildung beruht, muss dokumentiert und zugänglich gemacht werden. Allerdings hatte die Kommission eine Konstruktion vorgesehen, nach der Profiling grundsätzlich verboten und nur in bestimmten Ausnahmefällen erlaubt sein sollte. Der Parlamentstext dreht das Prinzip um und erlaubt Profiling, zur Entschädigung gibt es ein breit angelegtes Widerspruchsrecht. Der Unterschied mag auf den ersten Blick klein erscheinen und im Endeffekt auf dasselbe hinauslaufen. Das lässt aber außer Acht, dass die meisten Menschen davon vermutlich keinen Gebrauch machen, selbst wenn sie das Profiling stört. Bei allen Erleichterungen, die wir in dem neulich beschlossenen Text für das Widerspruchsrecht fordern, bleibt zu befürchten, dass nicht mehr davon Gebrauch machen werden als die, die heute schon das Auskunftsrecht wahrnehmen. Der Wechsel von einem opt-in zu einem opt-out Modell ist da wirklich nicht hilfreich.

Unter dem Strich haben wir, wie gesagt, einen guten Kompromiss gefunden, um die hoffentlich anstehenden Trilogverhandlungen mit Rat und Kommission noch in dieser Legislatur zu führen. Da an deren Ende die fertige Verordnung stehen soll, ist es in dieser Phase wichtig, dass viele Fachleute und Praktiker im Datenschutz den Text noch einmal genau unter die Lupe nehmen. Neben den genannten Punkten in den Artikeln 6 und 20 verdienen noch einige andere Punkte eine gründliche Prüfung. Dazu zählen meiner Ansicht nach die neue Rolle, die sogenannte pseudonyme Daten spielen werden, für die nun extra eine Definition aufgenommen und Regeln eingeführt werden sollen. Ein zweiter Punkt betrifft die Datentransfers in Länder außerhalb der EU. Hier wollen wir den neuen Artikel 43a einführen, der es verbietet, außereuropäische Gerichtsurteile und Verwaltungsbeschlüsse zu befolgen, wenn kein Rechtshilfeabkommen besteht. Damit werden einige Firmen sicher in Bedrängnis gebracht, wenn es ausdrücklich unmöglich sein wird, europäisches und amerikanisches Recht gleichzeitig zu befolgen, zumal Bußgelder drohen. Die tatsächlichen Folgen werden aber abzuwarten sein. In jedem Fall aber werden die Verhandlungen mit dem Ministerrat nicht einfach werden. Der erste folgende Schritt muss nun sein, den Rat auch tatsächlich an den Tisch zu bringen, und nicht die Verhandlungen auf 2014 zu verschieben. Da kann etwas Druck nicht schaden.



Birgit Sippel

Nationale Regierungen müssen bei der Datenschutzreform zeigen, dass es ihnen ernst ist mit (digitalen) Bürgerrechten

Ob beim Online-Banking, beim Versenden einer E-Mail oder bei der Nutzung sozialer Netzwerke – jeder von uns hinterlässt täglich einen digitalen Fußabdruck. Der Schutz dieser Daten ist das Grundrecht jedes EU-Bürgers, weswegen die derzeit noch gültige EU-Datenschutzrichtlinie aus dem Jahr 1995 dringend modernisiert werden muss. Bereits bevor die EU-Kommission im Januar 2012 ihren Vorschlag für eine Datenschutzreform – eine allgemeine Verordnung und eine Richtlinie für den Bereich Polizei und Justiz – vorgelegte, war klar: Die Verhandlungen würden nicht einfach werden. Für mich steht fest, dass das Recht auf Datenschutz nicht auf dem Altar der Interessen einiger Wirtschaftsvertreter geopfert werden darf. Die Politik muss den Mut haben, Bürgerrechte notfalls auch gegen wirtschaftliche Interessen durchzusetzen. Datenschutz und Wirtschaftsinteressen prinzipiell gegeneinander auszuspielen, wäre aber völlig falsch. Langfristig werden die Unternehmen von einem starken Datenschutz profitieren, weil die Kunden Vertrauen in die angebotenen Dienste haben müssen. Am 21. Oktober 2013 hat der Innenausschuss im EU-Parlament grünes Licht für die Datenschutz-Reform geben. Aber erst, wenn auch die Mitgliedstaaten im Rat ihre Position festgelegt haben, können die gemeinsamen Verhandlungen zwischen Kommission, Rat und Parlament beginnen. Wir wollen das Datenschutzpaket bis zu den Europawahlen im Mai 2014 unter Dach und Fach haben!

Auch wenn ich mir in einigen Bereichen, etwa beim Thema Beschäftigtendatenschutz, stärkere Formulierungen gewünscht hätte, stärkt die Parlamentsposition insgesamt die Rechte des Einzelnen. Der Bürger soll künftig jeder Datenverarbeitung im Vorfeld zustimmen müssen. Er erhält das Recht auf Information, Berichtigung und Löschung der Daten. Bislang verweisen Internetgiganten wie Google noch darauf, dass das EU-Datenschutzrecht für sie nicht gelte, weil sie in den USA ansässig seien. In Zukunft sollen hohe europäische Datenschutzbestimmungen auch für Unternehmen gelten, die ihren Sitz außerhalb der EU haben, deren Angebote sich aber an Verbraucher in der EU richten. Zudem soll es künftig für die Bürger eine zentrale Anlaufstelle für Datenschutzprobleme geben – in der Regel ihre nationale Datenschutzbehörde. Auch konnten wir Sozialdemokraten uns mit der Forderung nach hohen Strafen für Datenschutz-Sünder durchsetzen. Nur abschreckende Strafen stellen einen wirksamen Schutz vor Datenmissbrauch gerade durch große multinationale Konzerne dar. Sie sollen bis zu fünf Prozent des Jahresumsatzes oder 100 000 000 EUR umfassen.

Die Snowden-Enthüllungen über die massenhafte Bespitzelung europäischer Bürger unterstreichen die Bedeutung hoher europäischer Datenschutzstandards. Dabei geht es konkret um Bürgerrechte, (Meinungs-) Freiheit und Schutz der Privatsphäre. Es ist vor allem ein sozialdemokratischer Erfolg, dass der Datenaustausch mit Drittstaaten künftig strengeren Regeln unterworfen werden soll. Aber das beste Gesetz bietet keinen Schutz, wenn es von Geheimdiensten systematisch umgangen wird. Das Datenschutzpaket muss jetzt schnell verabschiedet werden; folgen muss eine Debatte über die Rolle von Geheimdiensten. Wir müssen europäische Grundrechte auch gegenüber den USA verteidigen. Die Forderung des EU-Parlaments nach Aussetzung des TFTP-Abkommens zum Rückgriff auf europäische Bankdaten war da ein wichtiger Schritt. Führende Politiker wie Parlamentspräsident Martin Schulz haben zudem laut über eine Unterbrechung der Verhandlungen über eine EU-US-Freihandelszone nachgedacht.

Die wieder stärker in den Fokus gerückte Debatte um den Schutz unserer Privatsphäre hat allerdings nicht dazu geführt, dass auch der geplanten Richtlinie für die Datenverarbeitung im Bereich der Strafaufklärung und -verfolgung genügend Aufmerksamkeit geschenkt wird. Dabei ist es gerade die Richtlinie, die die Mitgliedstaaten am liebsten beerdigen würden! Zur Unschuldsvermutung und dem Prinzip der Resozialisierung gehört, dass die Daten von Opfern und Beschuldigten während strafrechtlicher Ermittlungen, in Gerichtsverfahren sowie im notwendigen Umfang auch danach geschützt werden. Ich bin deshalb froh, dass die Mehrheit des Innenausschusses die Richtlinie gegenüber konservativen Erpressungsversuchen, insbesondere von Seiten des deutschen Innenministers Hans-Peter Friedrich, erfolgreich verteidigen konnte.

Die nationalen Regierungen müssen in den nun anstehenden Verhandlungen zeigen, dass es ihnen ernst ist mit (digitalen) Bürgerrechten, anstatt durch Tricks und Kniffe zu versuchen, das Datenschutzniveau weiter abzusenken. Die Ankündigung eines sog. Anti-Spionage-Abkommens ist KEIN Ersatz für eine effektive Datenschutzverordnung. Hier muss Herr Friedrich endlich seinen Widerstand aufgeben.



Axel Voss

Gesucht und gefunden? Die richtige Balance im Datenschutzrecht

Seit jeher kollidieren im Datenschutzrecht die Interessen zweier Parteien: Die Partei derer, die Daten nutzen wollen und sich einen möglichst freien Fluss dieser Daten wünschen und die Partei derer, die über diese Daten verfügen und diese bestmöglich geschützt wissen wollen. Dieses Spannungsfeld manifestiert sich in zahlreichen Einzelbeziehungen, sei es zwischen Unternehmen und Kunde, Bürger und Behörde, zwischen privaten Kontakten, internationalen Organisationen oder Staaten. Das Spannungsverhältnis lädt zur ideologischen Grundsatzfrage ein: Was kommt zuerst – Der Austausch von Daten oder der Schutz eben dieser? Ist Datenschutz ein „Supergrundrecht", das die Grundrechte, die mit ihm kollidieren, kompromisslos überstrahlt? Hat sich diese Balance in den 20 Jahren seit dem Bundesverfassungsgerichtsurteil zur Informationellen Selbstbestimmung 1983 unter dem Einfluss des digitalen Zeitalters verschoben?

Richtigerweise versucht die europäische Gesetzgebung nicht, diesen Widerspruch aufzulösen, sondern hat ihn bereits in der 1995er Datenschutzrichtlinie als inhärenten Widerspruch akzeptiert. Die dort festgeschriebenen „Twingoals" - oder zu deutsch „Zwillingsziele" - des europäischen Datenschutzrechts, nämlich die rechtliche Sicherstellung des individuellen Grundrechts auf Datenschutz einerseits und der freie Fluss von Daten in einem europäischen Binnenmarkt andererseits, stehen gleichrangig nebeneinander. Die Aufgabe, dieses Verhältnis im Rahmen der technisch und rechtlich notwendigen Überarbeitung der europäischen Datenschutzrichtlinie neu auszutarieren, sorgt bei den Gesetzgebern in Brüssel derzeit für einiges Kopfzerbrechen.

Unter dem Eindruck eines nicht nur freien, sondern unkontrollierten Datenmarkts im Internet und dem Weckruf von Edward Snowden hinsichtlich der Überwachungs- und Spionagepraktiken von Geheimdiensten, verstärkte sich der Eindruck, das „Ende der Privatsphäre" stünde unmittelbar bevor und der europäische Gesetzgeber müsse dringend zur Rettung ebendieser einschreiten. Richtig ist, dass für die neuen Datenmärkte auch neue, zeitgemäße Regeln geschaffen werden müssen. Die berechtigten Zwillingsziele jedoch auf das eine Ziel des maximalen Bürgerschutzes zu verengen, ist aus meiner Perspektive kurzfristig gedacht.

Das neue Recht muss das Vertrauen der Bürger zurückgewinnen und ihnen einen einfach zugänglichen und effektiven Datenschutz ermöglichen. Ebenso ist Europa aber auch auf Wachstumsimpulse im digitalen Markt angewiesen und kann sich eine Gesetzgebung, die vor lauter Datenschutzvorschriften Innovation behindert, schlichtweg nicht leisten. Mit Schrecken nehmen wir die Berichte über das Abzapfen privater Emaildaten aus der Hand von US-Unternehmen durch Geheimdienste wahr und schnell kommt die Frage auf, ob wir eine „Schengen-Cloud" oder ein „Deutsches Internet" schaffen müssen. Die Frage, die wir uns doch primär stellen müssen, ist die, warum es US-Unternehmen sind, die den Europäischen Markt dominieren und es europäische Alternativen nicht schon längst gibt.

Wer auf das zweite, gleichrangige Ziel verweist, den freien Fluss von Daten als Ware im Binnenmarkt, wird rasch mit dem Vorwurf konfrontiert, er hänge am Gängelband der Lobby und verliere das Wohl des Einzelnen aus dem Auge. Diesem Vorwurf liegt die Annahme zu Grunde, „der Bürger" wolle nur den höchstmöglichen Datenschutz. Vernachlässigt wird hier die Tatsache, dass ebendieser Bürger gerne von kostenfreien Emailkonten, kostenfreien Online-Informationsdiensten, günstigen Krediten und günstigen Versicherungstarifen profitiert und auch nicht zögert, diese zu nutzen. Alle genannten Beispiele basieren auf der Nutzung von Daten; das Emailkonto ist deshalb kostenfrei, weil es durch Werbung gegenfinanziert wird und sich Werbung umso mehr rechnet, je besser sie zugeschnitten ist. Die divergierende politische oder gar moralische Bewertung dieser Geschäftsmodelle darf nicht davon ablenken, dass sie vielfach durchaus akzeptierte, gelebte und gewünschte Praxis sind. Der Gesetzgeber tut daher gut daran, beide Ziele bei der Schaffung einer „Datenschutzgrundverordnung" im Auge zu behalten und gleichsam zu begrenzen.

Die genannten Aspekte haben in den Diskussionen, die wir im Kreis der Berichterstatter während der Verhandlungen im Parlament seit Januar 2012 geführt haben, eine zentrale Rolle gespielt. Die Frage, wie viel Datenschutz richtig ist und wie dieser konkret aussehen soll, war Gegenstand intensiver und teils harter Debatten. Ich bin überzeugt, dass in zahlreichen Artikeln schlussendlich eine gute Balance gelungen ist; die Tatsache, dass sich alle Fraktionen auf die Texte haben einigen können, ist für mich ein zusätzlicher Hinweis, dass der Ausgleich der Interessen im abgestimmten Text fair gelungen ist.

So haben wir bei den wichtigen Informationsrechten ein dreistufiges System gefunden, das den Betroffenen klarer und übersichtlicher als zuvor über seine Rechte aufklärt. Gleichzeitig wird unnötige Bürokratie vermieden und für den Wirtschaftsmotor der Klein- und Mittelständischen Unternehmen gibt es angemessene Ausnahmen.

Das „legitime Interesse" bleibt als Erlaubnistatbestand erhalten, findet aber seine Grenzen in den „gerechtfertigten/angemessenen Erwartungen" des

Betroffenen hinsichtlich einer Datenverarbeitung durch Dritte, der er nicht vorher zugestimmt hat.

Die Anreize für die Nutzung pseudonymisierter Daten werden gestärkt, besonders für den sensiblen Bereich der personalisierten Werbung im Internet. So konnte gleichzeitig das Wirtschaftsmodell erhalten werden und ein besserer Datenschutz eingebaut werden.

Der Ball liegt nun auf der Seite des Ministerrats. Ich hoffe, dass die Mitgliedstaaten dem gefundenen Ansatz folgen.



Peter Hustinx

EU-Datenschutzreform: Fortschritte in hitzigen Zeiten

Am Montag, dem 21. Oktober, hat der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) des Europäischen Parlamentes einen wichtigen und sehr begrüßenswerten Schritt zu einem stärkeren und effektiveren Datenschutz in Europa getan. Die Abstimmung des LIBE-Ausschusses über das Datenschutz-Reformpaket – das aus der vorgeschlagenen Datenschutz-Grundverordnung und der vorgeschlagenen Richtlinie zum Datenschutz für Zwecke der Strafverfolgung besteht – war bemerkenswert. Alle Kompromissänderungsanträge – die beiden Rechtsvorschriften galten – wurden mit sehr großen Mehrheiten angenommen. Dementsprechend wurden beide Rechtsvorschriften in vielfältiger Weise verbessert, auch wenn manche Einzelheiten in den abschließenden Phasen des Gesetzgebungsverfahrens noch einiger Aufmerksamkeit bedürfen.

Die Abstimmung des LIBE-Ausschusses hat den Weg für Verhandlungen über das Paket mit dem Rat geöffnet, sobald dieser dazu bereit ist, sich darauf einzulassen. Auch der Rat hat in seinen Diskussionen erhebliche Fortschritte erzielt, wenn auch mehr bei der Verordnung als bei der Richtlinie, aber zu beiden noch keinen umfassenden Standpunkt erreicht. Die LIBE-Abstimmung erhöht deshalb den Druck auf den Rat, zu Schlussfolgerungen zu gelangen, die eine Verabschiedung des Pakets vor den Parlamentswahlen im Frühjahr 2014 ermöglichen. Dieses Ziel hatte die Kommission vorgegeben, als sie das Paket im Januar 2012 vorstellte, und Frau Reding als zuständige Vizepräsidentin der Kommission hat hart daran gearbeitet, es zu erreichen.

Im Verlauf des Jahres 2013 ist die Debatte um das Reformpaket nach intensiver Lobbyarbeit hitziger geworden. Dennoch hat das Parlament einen effektiven internen Konsens zu den meisten wichtigen Fragen gefunden. Der Reformbedarf wurde nie infrage gestellt, aber es gab Diskussionen, zum Beispiel über das richtige Gleichgewicht zwischen europäischem und einzelstaatlichem Recht – mit einigem Raum für nationale Besonderheiten, aber auch mit einer angemessenen EU-übergreifenden Einheitlichkeit – und über das Erfordernis, für eine ausreichende Einhaltung zu sorgen, ohne übermäßigen Verwaltungsaufwand zu schaffen.

Die Snowden-Enthüllungen über die umfassende Überwachung und das Abfangen von Nachrichten durch die NSA haben zu einer weiteren Erhitzung geführt. Das hatte zur Folge, dass bestimmte Aspekte des Pakets mehr Aufmerksamkeit fanden als zuvor – Beispiele sind die Erweiterung des Geltungsbereichs von EU-Rechtsvorschriften auf Betreiber aus Drittländern, die auf dem europäischen Markt tätig sind, und Bestimmungen zur Verhinderung von unrechtmäßigen Datenübermittlungen in Drittländer. Zu einem gewissen Zeitpunkt konnte man sogar den Eindruck gewinnen, die Reform sei eine direkte Reaktion auf die NSA-Story. Das wichtigste Ziel des Pakets ist aber immer noch die Sicherung eines stärkeren, effektiveren und gleichförmigeren Datenschutzes in Europa.

Neue Berichte über eine umfassende Ausspähung in den EU-Mitgliedstaaten, darunter auch des Handys von Bundeskanzlerin Angela Merkel, kamen gerade vor dem Gipfeltreffen des Europäischen Rates am 24. und 25. Oktober ans Licht. Dadurch entstanden andere Prioritäten mit einer anderen Zielsetzung. Auf dem Gipfel ergriffen Deutschland und Frankreich die Initiative zu bilateralen Gesprächen mit den USA, um die gegenseitigen Beziehungen im Bereich der Informationssammlung „vor Jahresende“ zu klären. Andere EU-Länder sind eingeladen, sich dieser Initiative anzuschließen. Da die nationale Sicherheit in die ausschließliche Zuständigkeit der einzelnen Mitgliedstaaten fällt, wird dies aber nur in einem Anhang zu den Schlussfolgerungen des Rates erwähnt.

Im Hinblick auf die Datenschutzreform heißt es in den Schlussfolgerungen des Rates, dass die „rasche Verabschiedung“ eines soliden allgemeinen Rahmens für den Datenschutz in der EU für die Vollendung des digitalen Binnenmarkts bis 2015 von entscheidender Bedeutung sei. Die Kommission hat zu Recht auf eine ehrgeizigere Frist „bis Frühjahr 2014“ gedrängt, aber der schließlich erreichte Konsens führte zu einer flexibleren Formulierung. Diese lässt immerhin Raum für verschiedene Szenarien, darunter auch eines, nach dem der neue Rahmen im Verlauf des Jahres 2014 geschaffen werden sollte.

Es wäre deshalb außerordentlich wünschenswert, wenn sich der Rat dazu veranlasst sähe, seine Tätigkeit mit Hochdruck fortzusetzen, um die „rasche Verabschiedung“ eines soliden Rahmens zu sichern, wie sie der Europäische Rat ausdrücklich verlangt. Mit anderen Worten, es wird im Dezember Aufgabe des Rates „Justiz und Inneres“ sein, den Weg für produktive Verhandlungen mit dem Parlament freizumachen, die der LIBE-Ausschuss so nachdrücklich gefordert hat.



Peter Wedde

EU-Datenschutz-Grundverordnung – gut für den Beschäftigtendatenschutz?

Beschäftigtendatenschutz – eine endlose Geschichte

Das Thema „Beschäftigtendatenschutz“ wird in der BRD seit mehreren Jahrzehnten immer wieder und mit unterschiedlicher Intensität diskutiert, aber stets kontrovers. Trotz aller inhaltlicher Kontroversen besteht bei den an der Diskussion Beteiligten jedoch Einigkeit, dass normative Regelungen für den Bereich Datenverarbeitung im Rahmen von Arbeitsverhältnissen längst überfällig sind. Unterschiedlich sind allerdings die Zielrichtungen, die von den Diskutanten verfolgt werden: Arbeitgeber wünschen sich Erleichterungen bei der Verarbeitung personenbezogener Daten ihrer Belegschaften. Beschäftigte und ihre Interessenvertreter wollen vermeiden, das „Gläserne Beschäftigte“ und „Gläserne Belegschaften“ entstehen. Datenschützer streben einen vernünftigen Ausgleich der unterschiedlichen Interessen unter Wahrung eines datenschutzrechtlichen Mindeststandards an.

Nachdem die letzte schwarz-gelbe Bundesregierung ihren unausgewogenen Entwurf für ein Gesetz zum Beschäftigtendatenschutz nicht zuletzt auch unter dem Eindruck des im Internet deutlich gewordenen Protests vieler tausend Betroffener zurückgezogen hat, sind die Chancen für einen neuen Gesetzentwurf derzeit absolut offen. Auf einen an arbeitsrechtlichen Problemen orientierten Entwurf hoffen lässt die Information, dass die Arbeit an einem Beschäftigtendatenschutzgesetz nunmehr wieder da erfolgen soll, wo das Thema rechtlich auch hingehört: Im Bundesarbeitsministerium.

Dringend notwendig sind klare Regelungen für den Bereich des Beschäftigtendatenschutzes nach wie vor. Diese Feststellung leitet sich aus den zahlreichen Eingriffen in Persönlichkeitsrechte von Beschäftigten ab, die es täglich gibt. Unzulässige heimliche Videokontrollen finden in der betrieblichen Praxis nach wie vor ebenso statt wie ausufernde Gesundheitstests, unzulässiges Mitlesen von E-Mails oder Kontrollen des Internetverhaltens von Beschäftigten. Dass Datenschutzvorfälle der breiteren Öffentlichkeit nicht bekannt werden, liegt zumeist daran, dass sie nicht das personelle Volumen der großen Datenschutzskandale der Vergangenheit erreichen, sondern oft nur kleine Gruppen von Beschäftigten oder Einzelpersonen betreffen. Dies ändert indes nichts daran, dass es sich um unzulässige Eingriffe in Grundrechte der Betroffenen handelt.

Problematisch ist es darüber hinaus, dass Beschäftigte und ihre Betriebsräte in größeren Unternehmen bzw. in Konzernen vielfach mit der Situation konfrontiert werden, dass ihre personenbezogenen Daten irgendwo auf der Welt verarbeitet werden. Dieser Praxis steht auf der juristischen Seite das Problem gegenüber, dass die rechtlichen Möglichkeiten von Betriebsräten durch das Territorialitätsprinzip auf das Hoheitsgebiet der Bundesrepublik Deutschland beschränkt sind. Damit kommen grundlegende Rechtspositionen von Beschäftigten unter Druck, die sich insbesondere aus Grundrechten wie dem auf informationelle Selbstbestimmung oder dem auf Vertraulichkeit und Integrität informationstechnischer Systeme speisen.

Welche Gestalt nationale Regelungen zum Beschäftigtendatenschutz in der BRD annehmen, wird sich zeigen. Es ist aber zu erwarten, dass die Schaffung eines Gesetzes Eingang in eine Koalitionsvereinbarung finden wird. Allerdings könnte es passieren, dass weitere Aktivitäten so lange zurückgestellt werden, bis Klarheit über den Inhalt der derzeit als Entwurf vorliegenden EU-Datenschutz-Grundverordnung (EU-DS-GV-E) herrscht. Deshalb lohnt ein Blick auf die spezifischen Vorgaben, die sich zum Beschäftigtendatenschutz in der aktuellsten Entwurfsfassung der Verordnung[1] wiederfinden. Die folgende Darstellung beschränkt sich auf die Vorgaben in Art. 82 EU-DS-GV-E. Aus Raumgründen wird auf eine Bezugnahme zu den allgemeinen Regelungen der EU-DS-GV-E verzichtet, soweit sie nicht unumgänglich ist.

Beschäftigtendatenschutz auf europäischer Ebene

Eine explizite Regelung zum Thema Beschäftigtendatenschutz ist in Art. 82 EU-DS-GV-E enthalten. In der ursprünglichen Entwurfsfassung, die am 25. Januar 2012 vorgelegt wurde, beschränkten sich die entsprechenden Ausführungen in Art. 82 EU-DS-GV-E auf die Schaffung einer Ermächtigung für spezifische Regelungen zum Beschäftigtendatenschutz in den Mitgliedsstaaten. Damit wäre die gesetz-

geberische Autonomie der EU-Staaten weitgehend gewahrt geblieben. Auch die nationale Rechtsprechung hätte weiterhin uneingeschränkt Bestand gehabt.

Mit der aktuellen Fassung der EU-DS-GV-E vom 22. Oktober 2013 hat sich diese relativ offene Situation grundlegend verändert. Dies verdeutlicht schon das erheblich ausgeweitete Textvolumen der Vorschrift. Die Regelung stellt sich nunmehr nicht mehr nur als „Öffnungsklausel" für nationale Regelungen zum Beschäftigtendatenschutz dar, sondern enthält darüber hinaus zahlreiche rechtliche Vorgaben, die die Nationalstaaten unmittelbar binden würden.

Aus dem Regelungsgehalt des Entwurfs positiv hervorzuheben ist, dass durch die Vorgabe in Art. 82 Ziff. 1a EU-DS-GV-E festgeschrieben würde, dass eine Profilerstellung im Rahmen von Beschäftigungsverhältnissen ausgeschlossen ist. Damit sind die positiven Feststellungen aber schon fast beendet.

Zum vorliegenden Entwurfstext ist kritisch anzumerken, dass nationale Regelungen zum Beschäftigtendatenschutz aufgrund der Ergänzung im ersten Satz von Art. 82 Ziff. 1 EU-DS-GV-E unter Beachtung der Verhältnismäßigkeit erfolgen müssten. Dies könnte dazu führen, dass bei der Ausgestaltung nationaler Regelungen zugunsten von Arbeitgebern die Kosten des Beschäftigtendatenschutzes in die Waagschale geworfen werden könnten. Ergebnis wären möglicherweise Beschränkungen der Rechte der Beschäftigten. Die Liste der Kritikpunkte lässt sich fortsetzen.

- So eröffnet der letzte Satz von Art. 82 Ziff. 1 EU-DS-GV-E nationalen Gesetzgebern die Möglichkeit, Abweichungen vom Standard der Verordnung durch kollektive Vereinbarungen zuzulassen. Kämen entsprechende nationale Regelungen zustande, die „Abweichungen nach unten" erlauben würden, könnten Betriebsräte in der Folge unter Druck gesetzt werden, zwingende Vorgaben der EU-DS-GV-E durch den Abschluss von Betriebsvereinbarungen aufzuweichen.
- Durch Art. 82 Ziff. 1b EU-DS-GV-E würde eine freiwillige Einwilligung als Grundlage für Verarbeitungen in Beschäftigungsverhältnissen ausdrücklich zugelassen. Vollkommen ungelöst bliebe damit aber das Problem „erzwungener Freiwilligkeit", das in der Praxis häufig auftritt. Es ist insoweit absehbar, dass insbesondere Bewerberinnen und Bewerber sich mit umfangreichen Einwilligungsanforderungen potentieller Arbeitgeber konfrontiert sehen könnten.
- Herausragend kritisch ist es, dass die Regelung in Art. 82 Ziff. 1c (a) EU-DS-GV-E den Nationalstaaten ausdrücklich die Möglichkeit eröffnen würde, Verarbeitungen zu erlauben, die auf die Identifikation von schwerwiegenden Pflichtverletzungen von Beschäftigten zielen. Damit würde zugunsten der Arbeitgeber Möglichkeit etabliert, Daten von Beschäftigten im Verdachtsfall umfassend auswerten zu können. Das derartige Verarbeitungen an das Vorliegen von zu dokumentierenden tatsächlichen Anhaltspunkten gebunden wären, ist mit Blick auf die Rechtsprechung deutscher Arbeitsgerichte zum Thema „Verdachtskündigung" nur ein schwacher Schutz. Als „dokumentierter tatsächlicher Anhaltspunkt" würde möglicherweise ein „anonymer Hinweis eines Kollegen" ausreichen.
  Unklar bleibt in diesem Zusammenhang allerdings der Hinweis im letzten Satz von Art. 82 Ziff. 1c (a) EU-DS-GV, nachdem die Ermittlung „Sache der zuständigen Behörden" ist. Er könnte negativ so interpretiert werden, dass immer eine Strafanzeige erfolgen müsste.
- Durch die Regelung in Art. 82 Ziff. 1c (b) EU-DS-GV-E würde die offene Videokontrolle in Büros und Werkhallen weitgehend und pauschal legitimiert. Diese Feststellung lässt sich aus dem Wortlaut insoweit ableiten, dass entsprechende Maßnahmen lediglich in Räumen absolut verboten wären, die der privaten Lebensgestaltung der Beschäftigten dienen wie insbesondere Sanitär-, Umkleide-, Pausen- und Schlafräume. Hierzu ist anzumerken, dass die Installation von Videokameras in diesen Räumen in Deutschland auch schon heute unzulässig ist. Bezogen auf alle anderen Räume steht zu befürchten, dass durch die Formulierung in § 82 Ziff. 1c (b) EU-DS-GV-E insbesondere die restriktive Rechtsprechung des Bundesarbeitsgerichts zu diesem Thema, die eine Videoüberwachung von Beschäftigten nur ausnahmsweise als „ultima ratio" zulässt, ausgehöhlt werden könnte.
- Die Regelung in Art. 82 Ziff. 1c (c) EU-DS-GV-E zu ärztlichen Untersuchungen verzichtet auf eine Verankerung zur Erforderlichkeit und würde Untersuchungen damit in einem weiten Rahmen zulassen. Sie schreibt hingegen nicht zwingend fest, dass Arbeitgeber von Ärzten oder anderen an der Untersuchung beteiligten Personen nur eine Aussage zur Eignung erhalten dürften und nicht mehr.
- Auch die Regelung in Art. 82 Ziff. 1c (d) EU-DS-GV-E sieht bezogen auf die Verarbeitung von Telekommunikationsdaten ebenso wie Art. 82 Ziff. 1c (a) EU-DS-GV-E eine Berechtigung zur Verarbeitung vor, wenn es den Verdacht geht, dass schwerwiegende arbeitsrechtliche Pflichtverletzungen begangen worden sind. Insoweit wird auf die vorstehenden Aussagen verwiesen.
- Zu begrüßen ist das in Art. 82 Ziff. 1c (e) EU-DS-GV-E enthaltene und an Arbeitgeber gerichtete Verbot, „Schwarze Listen" zur Mitgliedschaft in Gewerkschaften oder politischen Parteien zu erstellen. Ein generelles Verbot der Verarbeitung dieser Daten durch Arbeitgeber fehlt hingegen. Dies lässt Interpretations- und Handlungsspielräume unterhalb „Schwarzer Listen" zu.
- Für die betriebliche Praxis in größeren Unternehmen und in Konzernen besonders bedeutsam ist die Schaffung eines Konzernprivilegs durch Art. 82 Ziff. 1d EU-DS-GV-E. Durch diese Regelung würde eine allgemeine Berechtigung zur unternehmensübergreifenden und weltweiten Verarbeitung von Beschäftigtendaten eingeführt, ohne dass zugleich den Betroffenen oder ihren kollektiven Interessenvertretungen adäquate Mitwirkungs- und Mitbestimmungsrechte eingeräumt werden. Folge dieser Regelung könnte in vielen Fällen sein, dass die Einhaltung von Betriebsvereinbarungen sich gerade in weltweit agierenden Konzernen nicht mehr wirksam kontrollieren lässt. Beschäftigtenrechte würden damit weitgehend ausgehöhlt.

- In ihren Auswirkungen unklar ist die Regelung in Art. 82 Ziff. 3 EU-DS-GV-E, durch den die Kommission ermächtigt wird, Maßnahmen zu erlassen, die auf die Datensicherheit zielen. Hierzu könnten indirekt auch Eingriffe in Persönlichkeitsrechte gehören.

Im Gesamtergebnis führt die Bewertung der Regelungen zum Beschäftigtendatenschutz in Art. 82 EU-DS-GV-E aus Sicht von Beschäftigten und Betriebsräten zu einer negativen Gesamtbilanz. Soweit in der Norm zwingende Vorgaben enthalten sind, lösen sie die Probleme nicht, die bezogen auf den Beschäftigtendatenschutz in Deutschland bestehen. Sie schaffen aber für bestimmte Verarbeitungen eine europaweite Rechtsgrundlage, die im Ergebnis hinter den durch das BDSG und die Rechtsprechung geprägten deutschen Standards zurück bleiben. Dies zeigt sich besonders deutlich an der Möglichkeit der Verarbeitung von Daten zur Identifikation von arbeitsrechtlichen Pflichtverstößen. Dass in Art. 82 EU-DS-GV-E in den Ziff. 1c (a) und (d) jeweils auf das Vorliegen von „schwerwiegenden Pflichtverstößen“ abgestellt wird, begründet mit Blick auf die Rechtsprechung zu den Möglichkeiten außerordentlicher Kündigungen auf der Grundlage von § 626 BGB keinen wirksamen Schutz der Beschäftigten. Als „schwerwiegend“ und damit kündigungsrelevant könnte von einem Arbeitsgericht beispielsweise ein mit einer unzulässigen Privatnutzung des Internets verbundene „Arbeitszeitdiebstahl“ qualifiziert werden.

Soweit dem nationalen Gesetzgeber durch Art. 82 EU-DS-GV-E Regelungsspielräume eröffnet werden, folgt hieraus kein Mehr an Beschäftigtendatenschutz. Dies verdeutlicht die ausdrückliche Möglichkeit nationaler Gesetzgeber, die Abweichung von Mindeststandards der EU-DS-GV-E auf Basis kollektiver Regelungen durch Gesetz zu ermöglichen.

Fasst man die Kritikpunkte zusammen, wird deutlich, dass der sich aus der vorliegenden Fassung von Art. 82 EU-DS-GV-E ableitende Beschäftigtendatenschutz aus der Sicht der Betroffenen nicht positiv zu bewerten ist. Würde die aktuell diskutierte Version der EU-DS-GV-E Wirklichkeit, könnte es passieren, dass sich in Deutschland Beschäftigte in einer Situation wiederfinden, in der ihre personenbezogenen Daten europaweit weniger geschützt wären als bisher und in der vom Bundesverfassungsgericht begründete Grundrechte wie das Recht auf informationelle Selbstbestimmung plötzlich grundlegend an Substanz verlören.

Betriebsräte müssten möglicherweise feststellen, dass bisher bestehende Mitwirkungs- und Mitbestimmungsrechte zum Schutz von Beschäftigten vor unzulässigen oder ausufernden Verhaltens- und Leistungskontrollen durch die EU-DS-GV-E reduziert würden.

Damit beantwortet sich die in der Überschrift gestellte Frage schon fast von selbst: Die EU-Datenschutz-Grundverordnung ist in der aktuellen Entwurfsfassung sicher nicht gut für den Beschäftigtendatenschutz.

1 Die folgenden Ausführungen beziehen sich auf die „Inofficial Consolidated Version after LIBE-Committee Vote provided by the Rapporteur“ vom 22. Oktober 2013 (http://ddma.nl/wp-content/uploads/2013/10/DPR-Regulation-inofficial-consolidated-LIBE.pdf)

Douwe Korff



Surveillance and the EU general data protection regulation: Possibilities, limits and obstacles

The global surveillance scandal

Since May this year, the UK Guardian, Der Spiegel and other papers have bit-by-bit revealed much (though still far from all) of the massive world-wide surveillance operations of the U.S. National Security Agency and the UK's GCHQ.[1] Although the revelations continue, it is clear that in this unprecedented global spying scheme the USA and the UK cooperate extremely closely, not only with their usual “5EYES” allies, Australia, New Zealand and Canada, but also with the secret intelligence agencies of many other “friendly” countries, including Germany.

Part of the scheme onsists of the tapping into the main cables through which much of the Internet traffic is routed. This applies not only to the very important transatlantic submarine cables, but also to other cables through which data travel that comes from or goes through politically - or commercially - sensitive areas. Thus, it was reported that the UK's GCHQ maintains such a capability in the Eastern Meditterraean, to spy on traffic to and from (and within) the Middle East, and that the NSA spied on the European institutions from NATO's Brussels headquarter. Reportedly, the main Internet exchange in Frankfurt a/M has also been compromised. There is also extremely widespread spying on mobile telecommunications data - not just by listening in to mobile phone exchanges within direct reach of UK and US embassies (including those in Berlin, near the Chancellery), but also by accessing the global mobile phone infrastructure, and in particular the GRX routers.[2] Moreover, the secret agencies have created security loopholes in to the

until recently deemed secure systems and servers of the major Internet "giants" such as Google, Facebook, etc., through which they can access their data too.

The NSA and GCHQ are trying to hold effectively all the data that flows through these channels for a few days, in massive "buffer" servers. The incredibly vast amounts of data thus collected are queried by analysts on the basis of "selectors" such as IP addresses, names or word combinations, or other factors. Presumably these analyses are dynamic, in that the systems can themselves create, by means of artificial intelligence such as are also used in commerial data mining, more sophisticated profiles that can be used for further, supposedly more effective searches.[3]

The targets of this surveillance are not only terrorists, paedophiles and drug barons: the legal definition of "foreign intelligence" in the U.S. FISAA Act and the wide mandate of the UK intelligence services clearly also allow (and are certainly interpreted as also allowing) the use of the above mining technologies to obtain general information on political activities (including entirely peaceful and lawful activities) of "activist" groups and individuals, commercial entities (to provide home companies and their governments with advantages in negotiations that affect the "economic well-being" of the country), and indeed on the activities and intentions of other governments and heads of governments, including those of close allies, and of intergovernmental organisations, including OPEC and the UN.

Suspicionless mass surveillance is unlawful under international human rights and data protection law - but the USA and the UK are unwilling to abandon it

In a hearing of the European Parliament's LIBE Committee's inquiry into surveillance, Prof. Martin Scheinin, Judge Bostjan Zupancic of the European Court of Human Rights and I all stressed that suspicionless mass surveillance is in fundamental breach of international human rights and data protection law. In particular, as Judge Zapan expressly confirmed, the protection of privacy, private life and private communications under Art. 8 ECHR is already "interfered with" when data on one's communications are collected - the protection of the article does not just kick in when personal data are accessed or used, but applies from the very moment of collection.[4]

The "hoovering-up" of the massive amounts of data on everyone's Internet searches, e-communications and social network activities, "just in case" there is information "of interest" in the data mountain, is of course also fundamentally contrary to the most basic data protection principles of purpose-limitation, data-minimisation, necessity and proportionality, etc.

Yet neither the USA nor the UK Governments seem to be prepared to abandon the schemes. Rather, they insist all the data collecting is lawful and necessary for "foreign intelligence" or "national security" purposes. The head of GCHQ, when (very gently) questioned by the Government-selected UK Parliamentary Intelligence and Security Committee, said they needed to collect all the hay in the haystack, in order to find the needles they were looking for.[5]

The UK Government also argues that because matters of "national security" are outside EU competence, the EU has no right to question these activities. On that basis, the UK refused to appear before the European Parliament's committee of inquiry.

After a brief discussion of the new EU data protection rules-in-the-making, this article examines this claim of a full exemption, and concludes that it is not a valid claim and that the EU has the right to ask questions about the surveillance programmes. In some brief concluding remarks, I note some main data processing operations that are, and must remain, subject to the EU rules.

The new EU data protection rules

As Peter Schaar makes clear in another contribution to this journal, there are some very positive aspects to the amended version of the General Data Protection Regulation (hereafter: GDPR or "the Regulation"), adopted by the European Parliament after good work by the LIBE Rapporteur, Jan Albrecht. Peter mentions inter alia the application of the Regulation to non-EU-based controllers who "monitor" data subjects in Europe (even if they are not established in the EU), the improved provisions on consent and stronger limitations on profiling (including the requirement, first proposed by EDRi on the basis of my own suggestions, that controllers who use profiling must ensure that this does not result, even unintentionally, in discrimination against people on grounds of race, religion, sexual orientation, etc.). The latter is of particular importance because the "keyword analyses" carried out in the spying programmes in effect rely on profiling.

Peter Schaar rightly places special emphasis on the proposed new Article 43a, that says, first of all, that judicial or administrative orders from third countries requiring the handing over of personal data may only be complied with by entities subject to the Regulation - i.e., in particular, private entities - if they are based on a mutual legal assistance treaty (known as MLAT) or another international agreement. The article also stipulates that (apparently, even if there is an MLAT or other treaty in place), the requested entity must inform the relevant data protection authority and obtain the prior authorisation of the authority before the data can be legally handed over.

I would add to this the crucially important "consistency mechanism", under which DPAs and the new European Data Protection Board EDPB (the successor to the Article 29 Working Party) can ensure that issues that affect data subjects in several or all EU countries will be addressed at the European level if there are doubts about the proposed application of the rules by the "lead authority".

The "national security" exemption[6]

"National security" is exempted from EU competence. As Article 4(2) TEU puts it:

"[N]ational security remains the sole responsibility of each Member State."

Art. 73 TFEU adds that "[Member States may] organise between themselves and under their responsibility such forms of cooperation and coordination as they deem appropriate between the competent departments of their administrations responsible for safeguarding national security." - but if anything, this merely underscores that the matter is the responsibility of the States, and not of the Union.

In other words, on the face of these

texts, it would appear that the EU has no competence at all on matters relating to national security; that those matters remain the sole responsibility of the States; and that the Member States are also free to organise any cooperation between themselves - and with third countries - as they deem fit.

Moreover, since national security is outside EU competence and thus outside EU law, it would appear to follow that the Charter FR (which is EU law) does not apply to anything the MSs do (either by themselves or in some form of cooperation, be that within the EU or with third countries) in relation to national security; and that the ECJ also has no jurisdiction over such matters at all.

The United Kingdom has relied on this exemption to refuse to appear before the LIBE Committee inquiry to explain its own GCHQ surveillance; and to try and prevent even the Council from expressing any views on the NSA or GCHQ activities.

However, that is an over-statement of the legal position that threatens the fundamental rights of all EU citizens.

First of all, Article 4(2) begs the question of what exactly is covered by the term "national security", and whether it is solely left to the Member States to define this concept as they like. Second, the exemption must be seen in the context of closely-related activities that are undoubtedly within the EU's competences.

On the first point, is should be noted that there is no generally-accepted, binding definition of the concept of national security in international law. However, it is a widely agreed principle of treaty law that exceptions to treaty obligations must be interpreted narrowly; even if one can argue about the application of this principle in general public international law,[7] this certainly applies to provisions that create exemptions from human rights obligations, as the European Court of Human Rights has consistently stated. With regard to national security, this approach is confirmed by the Johannesburg Principles, adopted on 1 October 1995 by a group of experts in international law, national security, and human rights convened by Article 19, the International Centre Against Censorship, in collaboration with the Centre for Applied Legal Studies of the University of the Witwatersrand, in Johannesburg, and endorsed by Mr. Abid Hussain, the UN Special Rapporteur on Freedom of Opinion and Expression, in his reports to the 1996, 1998, 1999 and 2001 sessions of the United Nations Commission on Human Rights, and referred to by the Commission in their annual resolutions on freedom of expression every year since 1996.[8] They stipulate the following, in Principle 2, "Legitimate National Security Interest":

a A restriction sought to be justified on the ground of national security is not legitimate unless its genuine purpose and demonstrable effect is to protect a country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force, whether from an external source, such as a military threat, or an internal source, such as incitement to violent overthrow of the government.

b In particular, a restriction sought to be justified on the ground of national security is not legitimate if its genuine purpose or demonstrable effect is to protect interests unrelated to national security, including, for example, to protect a government from embarrassment or exposure of wrongdoing, or to conceal information about the functioning of its public institutions, or to entrench a particular ideology, or to suppress industrial unrest.

The same applies to restrictions claimed to be imposed for national security reasons, but which in reality seek to provide the country concerned with an advantage in diplomatic negotiations, or an economic advantage for itself or the country's industries.

Also important in relation to the EU is the fact that the European Commission appears to suggest that anti-terrorist measures should primarily be taken within a "justice and home affairs"/police and criminal law framework, rather than within a "national security" one, also and in particular in relation to cross-border data collection:

"The European Commission will also emphasise that [the EU-USA Mutual Legal Assistance Agreement (MLA) in force since February 2010] is a useful tool and should be the principal channel used for judicial cooperation in criminal matters, for example when the U.S. would like to request data of EU citizens outside the U.S. territory."[9]

Here, it suffices to note that the fight against global and domestic terrorism cannot be simply claimed by States as (only) matters of "national security".

The above contrasts with the extremely wide concepts used by the USA and the UK in relation to their PRISM, TEMPORA and other surveillance programmes:

In the UK, there is no formal definition of "national security" in any statute or judicial decision. However, it is acknowledged that the concept has been expanded and is now very broad, to include not just military threats, espionage, etc., but also pandemics, cyberthreats, matters relating to energy security, etc.[10] In fact, GCHQ's surveillance powers go even beyond this: surveillance warrants such as those presumably used to legitimise TEMPORA can be issued when the Secretary of State "believes" they are necessary and proportionate:

a in the interests of national security [as widely defined: see above];
b for the purpose of preventing or detecting serious crime;
c for the purpose of safeguarding the economic well-being of the United Kingdom [provided the targets are outside "the British Islands"]; or
d...

(Regulation of Investigative Powers Act, s. 5. Para. (d) concerns mutual assistance in criminal matters, but warrants authorising mass surveillance cannot be issued to that end)

"National security" also covers assistance to foreign governments in order to maintain good relations with them. The reference to the "beliefs" of the Secretary of State means that the test is almost entirely a subjective one. Moreover, the warrants are issued in secret and are not subject to judicial oversight.[11] The non-judicial oversight mechanisms have obviously not resulted in restraints on the non-targeted data collection.

As for the USA, as Caspar Bowden in particular has shown in his excellent study for the EU, the U.S. FISAA Act, as amended, allows for effectively unlimited surveillance on non-US citizens living outside the USA for the purpose of obtaining "foreign intelligence information"; and the definition of "foreign intel-

ligence information" in FISAA, as amended, now includes any information with respect to a foreign-based political organization or foreign territory that „relates to the conduct of the foreign affairs of the United States". (See FISA §1801(a) & (e)). Consequently, it is lawful for the NSA under U.S. Law to conduct purely political or economic surveillance on foreigners‘ e-communications data and their data accessible in US Clouds.

As further discussed below, in my opinion the Court of Justice of the EU, the European Commission and the European Parliament are all competent to assess whether the UK's surveillance activities in particular are covered by the "national security" exemption in the treaties, and to rule that certain activities - e.g., purely political or commercial spying - are not.

On the second issue (the relationship between the "national security" exemption and matters that are within EU competences), it is important to note that as part of the EU's Common Foreign and Security Policy (CSFP) the Union is required to "safeguard its [i.e., the Union's] values, fundamental interests, **[internal] security,** independence and integrity" and to "strengthen **international security**" (Art. 21(2)(a) & (c) TEU); and that Article 4(2)(j) TFEU provides for "shared competence" between the Union and the MSs in respect of the area of "freedom, **security** and justice", covered by Part Three, Title V, TFEU, including in relation to the fight against crime, racism and xenophobia (see Art. 67(3) and against "**terrorism** and related activities" (see Art. 75).

In other words, Member States may have sole competence in relation to their own national security, but the Union has shared competence with the Member States when it comes to the Union's own internal security, and in relation to crime and terrorism; and under the CFSP the Union also has its own competences in relation to international security and terrorism.

There are clearly considerable overlaps between these matters - and that has implications for the scope of the "national security" exemption. In particular, the Member States' "national security", each Member States' "internal security", the Union's "internal security", and "international security" cannot be separated from each other, nor from JHA action, in particular in relation to "terrorism and related activities" (or international crime, or extremism or xenophobia); and the duties and responsibilities that Member States have in relation to the latter matters impact on the autonomy they enjoy in relation to the first.

Specifically, it follows from general law on treaties that MSs may not invoke Art. 4(2) TEU in such a way as to negate or undermine the shared competences of the EU in relation to internal security, crime and terrorism. Member States' "autonomous" actions to protect their own national security must respect, and tie in with, their joint or cooperative or coordinated actions with other Member States in relation to the EU's own internal security, the joint security of all the Member States, and the joint fight against international crime and terrorism.

Member States may also not use their powers in the exempt area to negate or undermine the Union's general aquis, including fundamental rights:[12]

"National measures which seek to maintain national security may not interfere with the fundamental freedoms and, insofar as they fall within the scope of EU law, must respect fundamental rights as understood in the EU legal order."

In my opinion, it follows from the above that the EU institutions are legally allowed to assess, within their own competences:

I whether the UK's surveillance programmes, and its data exchanges/cooperation with the USA, are limited to the protection of "national security" in the sense in which that term must be understood in international and EU law;

II even if they are so limited: whether they do not unduly affect actions lawfully taken by the Union (or by its Member States acting jointly under Union law) in relation to internal or international security, and/or in relation to the fight against terrorism; and/or whether they do not unduly affect the Union's fundamental freedoms;

III to the extent that they are not limited to the protection of "national security" as understood in international and EU law: quite broadly, whether those programmes are compatible with Union law (since the Art. 4(2) TEU exemption does not apply);

IV specifically, the latter would include competence to assess whether the programmes meet the Union's privacy and data protection requirements; and

V in relation to the U.S.'s surveillance programmes, whether the USA is acting in contravention of the EU's data protection rules in any activity carried out in the EU; and whether the "Safe Harbor" and other EU-USA arrangements relating to personal data are actually safe and appropriate.

Concluding remarks

After adoption of the Regulation and the new Directive, there will still be several different data protection regimes:

- processing of personal data by private entities established in the EU, and by private entities not established in the EU that offer goods and services to data subjects in the EU, or that "monitor" data subjects in the EU, will be subject to the Regulation;
- processing of personal data by public entities carrying out activities within Union law will also be subject to the Regulation, except that:
- processing of personal data by "competent public authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties" will be subject to the new Directive;
- processing of personal data by the EU institutions themselves will be subject to Regulation (EC) No 45/2001;
- processing of personal data by the Member States when carrying out activities relating to the EU's Common Foreign and Security Policy, while subject to Union law, is exempt from the Regulation and the Directive and not subjet to any special data protection rules - but it is subject to the Charter of Fundamental Rights and must therefor respect privacy and comply with basic data protection principles; and
- processing of personal data by the Member States in relation to national security will not be subject to the EU data protection rules at all - except for the caveats outlined above: that the EU can judge whether any processing in this connection that is claimed to be for national security purposes actually

serves those purposes as properly (and narrowly) defined, and whether the processing is compatible with the rules on issues that are within the EU's competences.

What will be crucial in this regard is for the EU to make absolutely clear that any disclosure of personal data by any entity subject to any of the above-mentioned EU data protection regimes to any entity subject to any of the other EU data protection regimes, or to any entity not subject to any of the EU data protection regimes - including in particular national security agencies - is subject to the rules on the processing of personal data and on the disclosing of such data in the instrument that applies to the disclosing entity, even if the **obtaining and further processing** of the same data by the other entity (the recipient of the data) is subject to a different regime (and must therefore comply with the rules for that regime). In particular, any disclosures of personal data by a private sector entity subject to the new Regulation to any national security agency, either in the same country, or in another EU country, or (especially) in a non-EU country, is subject to the rules on disclosures in the Regulation; and any disclosures of personal data by an agency subject to the new Directive to any national security agency is subject to the rules on disclosures in the Directive - even if the collecting of the data by the relevant national security agency is not subject to either of those instruments.

The surveillance programmes so bravely exposed by Edward Snowden are a threat to our societies and our democracies. As the German Constitutional Court said in its famous Census judgment: individuals who must fear that all that they do is recorded by the State will be discouraged from exercising their fundamental rights of freedom of communication, association and expression: such a society is no longer free and democratic. NSA and GCHQ have realised the nightmare. We must wake our societies up and stop the surveillance. Strong European data protection rules, meeting at least the German constitutional requirements (as also reflected in European human rights law) are required to achieve this.

NOTES:

1 See: http://www.theguardian.com/world/the-nsa-files

2 See: http://www.spiegel.de/international/europe/interview-telecom-security-expert-philippe-langlois-on-gchq-spying-a-933870.html

3 See the witness statement of Ian Brown in the ECHR case of Big Brother and Others v. the UK, at:
https://www.privacynotprism.org.uk/assets/files/privacynotprism/IAN_BROWN-FINAL_WITNESS_STATEMENT.pdf
The application itself (Application No. 58710/13) can be found here:
https://www.privacynotprism.org.uk/assets/files/privacynotprism/496577_app_No_58170-13_BBW_ORG_EP_CK_v_UK_Grounds.pdf

4 See the Note and the powerpoint slides prepared for my presentation to the inquiry of the European Parliament's Civil Liberties Committee into the NSA/GCHQ spying scandal (session on the legal issues, Brussels, 14 October 2013), and the video recording of my presentation and of the other two experts:
The Note and the powerpoint slides submitted to the Committee are available here:
http://www.europarl.europa.eu/meetdocs/2009_2014/organes/libe/libe_20131014_1500.htm
The video recording is here (my presentation starts at 55 minutes into the hearing):
http://www.europarl.europa.eu/ep-live/en/committees/video?event=20131014-1500-COMMITTEE-LIBE

5 See the video recording of the session here: http://www.parliamentlive.tv/Main/Player.aspx?meetingId=14146
The (so far uncorrected) transcript can be found here:
https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20131107_ISC_uncorrected_transcript.pdf?attachauth=ANoY7cp2aR_LqRd4x_9wbKeAqbrlwnCj8Bpjtlco7AcFXGvagOM6_RW2Ksh_rp95-mw8fo9jiGwa_6rc7gcrgYcDgx5l3jAuuIzuCIdoyVBxvZqCQfMA4jBaQZEF-TRU5onUOEAlqdniFVJGtp9cneW_MlOEAaZpyufM8hpqiDGHf-bqKXMEApt7X8rhEtHoFm0ANS08vt-gI0MCc2S9laJypMdUwY_OVAJPsn4365pjdJe2A7N0SL5x5JrUNuJiJTfEtyUv3sqV9BI&attredirects=0
The reference to the haystack is on p. 13, as follows: SIR IAIN LOBBAN: "... If you think of the internet as an enormous hay field, what we are trying to do is to collect hay from those parts of the field that we can get access to and which might be lucrative in terms of containing the needles or the fragments of the needles that we might be interested in, that might help our mission.
When we gather that haystack, and remember it is not a haystack from the whole field, it is a haystack from a tiny proportion of that field, we are very, very well aware that within that haystack there is going to be plenty of hay which is innocent communications from innocent people, not just British, foreign people as well. And so we design our queries against that data, to draw out the needles and we do not intrude upon, if you like, the surrounding hay. We can only look at the content of communications where there are very specific legal thresholds and requirements which have been met. So that is the reality. We don't want to delve into innocent e-mails and phonecalls."
The reason Sir Iain is claiming that they only collect "a tiny proportion of [the hay-field", is that the systems automatically exclude communications that are of no interest, such as spam or music downloads. However, all real communications between real individuals that flow through the compromised systems are hoovered up. Note the suggestion that communications that are not singled out by the selectors are "not intrude[d] upon". The "legal thresholds and requirements", moreover, are actually euphemisms for these very selectors. What Sir Iain is saying is that they will look at any communication that is flagged up as "of interest" on the basis of the selectors, and that that is perfectly acceptable - and legal under UK law.

6 This sub-section draws on my presentation to the EP's LIBE Committee (see footnote 4, above).

7 See Luigi Crema, Disappearance and New Sightings of Restrictive Interpretation(s), EJIL Volume 21 (2010), Issue 3, pp. 681 – 700, available at:
http://ejil.oxfordjournals.org/content/21/3/681.full

8 See: http://www.refworld.org/docid/4653fa1f2.html.

9 Memo on EU-U.S. Justice and Home Affairs Ministerial meeting: 18 November 2013 in Washington, D.C., available at:
http://statewatch.org/news/2013/nov/eu-usa-ministerial-18-nov-13-washington.pdf
Press release at:
http://europa.eu/rapid/press-release_MEMO-13-1010_en.htm

10 See the ECtHR application by Big Brother Watch and Others v. the UK (ffotnote x, above), paras. 105 – 112, with references to case-law and parliamentary debates.

11 On the deficiencies in the UK surveillance oversight regime, see the ECtHR application Big Brother and Others v. the UK (footnote 3, above), passim.

12 Diamond Ashiagbor, Nicola Countouris, Ioannis Lianos (Eds.), The European Union After the Treaty of Lisbon, Cambridge University Press, 2012, p. 57.

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

Stille SMS bei Sicherheitsbehörden nehmen massiv zu

Gemäß einer Antwort der Bundesregierung auf eine Anfrage des Linken-Abgeordneten Andrej Hunko haben Bundespolizei (BPol), Bundeskriminalamt (BKA), Zoll und das Bundesamt für Verfassungsschutz (BfV) in der ersten Hälfte des Jahres 2013 insgesamt 264.648 Handy-Ortungen mit Hilfe sogenannter stiller SMS durchgeführt. Im gesamten Jahr 2012 waren es 328.572. Wie oft der Bundesnachrichtendienst stille SMS zur Ortung von Mobiltelefonen verschickt hat, soll die Öffentlichkeit nicht erfahren; diese Angaben sind als Verschlusssache eingestuft. Der Geheimdienst der Bundeswehr verschickte laut der Antwort nur eine stille SMS im vergangenen Jahr.

Hunko kritisierte die Zunahme der Überwachung: „Berichte über die zunehmende Überwachung digitaler Verkehre untergraben das Vertrauen in die Freiheit des Internet und der Telekommunikation.“

Versand „stiller SMS“

Jahr	2012 (gesamt)	2013 (1. Halbjahr)
BfV	28843	28472
BKA	37352	31948
BPOL	63354	65449
Zoll	199023	138779

Beim Versand einer stillen SMS merkt der Betroffene in der Regel nicht, dass er kontaktiert wird. Bei der Nachricht handelt es sich um bloße Steuerbefehle; das Telefon antwortet dem Provider unbemerkt. Dieser kann dann anhand dieser Daten den Aufenthaltsort des Telefons an die Behörden weitergeben. Um die Bewegungen einer Person aufzuzeichnen, können beispielsweise mehrere dieser SMS hintereinander verschickt werden. Neben den Bundesbehörden verschicken auch die Polizeibehörden in den Ländern stille SMS. In Nordrhein-Westfalen beispielsweise waren das im Jahr 2010 schon rund 250.000, wie eine Anfrage der Linken im Landtag enthüllte (Deutsche Ermittler nutzen immer häufiger verdeckte Handy-Ortung, www.spiegel.de 06.09.2013).

Bund

Personaldatenpanne bei der Telekom

Bei der Telekom hat es trotz verschärfter Datenschutz-Vorgaben eine Panne mit Personaldaten in einem IT-System gegeben: Ein begrenzter Kreis von Mitarbeitenden hatte seit 2002 Zugriff auf personenbezogene Daten von fast allen 120.000 Beschäftigten in Deutschland gehabt, die in dem System eigentlich hätten anonymisiert werden müssen. So konnten Angaben wie etwa Namen, Adressen, Gehälter oder Personalnummern eingesehen werden. Eine missbräuchlich Nutzung der Personaldaten hat es nach Angaben eines Konzernsprechers nach dem bisherigen Kenntnisstand des Unternehmens nicht gegeben: „Wir bedauern sehr, dass wir unseren eigenen hohen Ansprüchen beim Schutz von Mitarbeiterdaten selbst nicht gerecht geworden sind.“ Der Vorstand stehe in enger Zusammenarbeit mit dem Betriebsrat und habe sich bei den Mitarbeitenden entschuldigt.

Eine unabhängige externe Wirtschaftsprüfungsgesellschaft soll herausfinden, wie es zu der Datenpanne kommen konnte. Der Betriebsrat will diese Arbeiten durch einen eigenen Anwalt begleiten lassen. In den vergangenen Jahren hatte Konzernchef René Obermann den Datenschutz im Unternehmen kräftig ausgeweitet und sogar ein Vorstandsressort eingerichtet. Vor drei Jahren wurde ein ehemaliger Sicherheitschef zu einer Haftstrafe verurteilt, weil er maßgeblich an der illegalen Ausspionierung von Journalisten und Arbeitnehmervertretern im Aufsichtsrat beteiligt gewesen war (Telekom-Mitarbeiter konnten Gehälter von 120.000 Kollegen einsehen, www.sueddeutsche.de 28.08.2013).

Bund

Rechtsanwälte gegen Totalüberwachung

Eine Gruppe von Rechtsanwälten hat innerhalb weniger Tage erreicht, dass tausende Juristen und andere Bürger eine Erklärung gegen die Überwachung durch die die US-amerikanischen und britischen Geheimdienste NSA und GCHQ unterschrieben.

Die Initiative „Rechtsanwälte gegen Totalüberwachung“, zu der auch die Bundestagsabgeordneten Burkhard Müller-Sönksen und Konstantin von Notz gehören, will, so ihre neue Webseite „rechtsanwaelte-gegen-totalueberwachung.de“, „ein Zeichen der Anwaltschaft gegen Totalüberwachung setzen“ und die Bevölkerung „sensibilisieren“. Die Freiheit jedes Einzelnen sei akut bedroht, „doch in der Politik und in der Gesellschaft bleibt es beunruhigend still. Das wollen wir ändern.“ Vor den Rechtsanwälten hatten sich schon als Berufsstand deutsche Schriftsteller um Juli Zeh zusammengetan und von der Bundeskanzlerin gefordert, die Affäre aufzuklären und das Spionieren nicht billigend in Kauf zu nehmen. Die Anwälte zeigen sich mit der Schriftstellergruppe solidarisch und schickten am 02.10.2013 einen Brief an den amerikanischen Botschafter in Berlin, in dem sie um Auskunft zum Fall

Ilja Trojanow baten, einem den Initiatoren des Autoren-Briefes, dem offensichtlich wegen seiner Kritik an der NSA die Einreise in die USA verwehrt wurde. Oliver Pragal, Gründungsmitglied der Anwaltsinitiative, erläuterte: „Die Kampagne von Juli Zeh ist mit unserer vergleichbar, deshalb fragen auch wir uns, ob wir zukünftig Probleme bekommen könnten, wenn wir in die USA einreisen wollen."

In der sogenannten Hamburger Erklärung steht, dass die von Edward Snowden offengelegte digitale Totalüberwachung „ein historisch beispielloser Angriff auf das verfassungsmäßige Grundrecht auf Privatsphäre" sei, was „die zentralen Funktionsbedingungen unserer freiheitlich-demokratischen Gesellschaftsordnung" gefährde. Die Überwachung ermögliche Wirtschaftsspionage und die Erpressung von Politikern oder Managern. Sie zerstöre das Vertrauen der Bürger in „Berufsgeheimnisträger", also beispielsweise in Ärzte, Journalisten, Seelsorger oder eben Anwälte. Gründungsmitglied Wolfgang Prinzenberg: „Die Menschen werden sich ganz genau überlegen, was sie schreiben und sagen, und das wäre das Ende einer unbeschwerten, unbelasteten Auseinandersetzung in unserem Land."

Die Juristen fordern die Bundesregierung auf:

- zu erklären, dass die anlass- und verdachtsunabhängige Totalüberwachung der deutschen Bevölkerung eine "krasse Verletzung von Grundrechten" darstelle,
- alle Maßnahmen auf EU-Ebene gegen Großbritannien zu prüfen,
- alle Verhandlungen mit den USA über ein Freihandelsabkommen auszusetzen und die "Safe-Harbour-Abkommen" sowie die Verträge zum Austausch von Fluggastdaten zu kündigen – bis die Überwachung beendet werde,
- sämtliche Standorte der NSA in Deutschland zu schließen,
- die Netze und Netzwerkeinrichtungen in Deutschland zu prüfen, um ein Abzapfen von Daten auszuschließen,
- eine strengere Kontrolle der deutschen Nachrichtendienste zu veranlassen,
- dafür zu sorgen, dass Berichte vor Kontrollgremien künftig mit Vollständigkeitserklärungen unter Eid erstattet werden müssen,
- die Verwendung von Programmen wie XKeyscore zu stoppen oder diese zumindest unter eine strenge Prüfung zu stellen.

Die Erklärung soll mit der online zu unterzeichnenden Unterschriftenliste der Bundesregierung übergeben werden (Horchert, Protest gegen Prism und Co.: Aufstand der Anwälte, www.spiegel.de 04.10.2013).

Bundesweit

Auskunfteimarkt öffnet sich für Privatkunden

Auskunfteien stellten ihre Daten zur Kreditwürdigkeit lange Zeit nur Gewerbetreibenden zur Verfügung, doch in jüngerer Zeit versuchen einige von ihnen, mit Privatpersonen eine neue Kundengruppe zu erschließen. Diese können z. B. interessiert sein zu erfahren, wie es um die Bonität eines Bauträgers bestellt ist, mit dem sie ein privates Bauvorhaben durchführen.

Sommer 2013 wurde die Internetseite monetas.de freigeschaltet, auf der KundInnen Einzelauskünfte oder Datenpakete über mögliche Geschäftspartner erwerben können. Dahinter steckt die schwedische Auskunftei Bisnode, die in Deutschland bis vor kurzem unter der Marke Hoppenstedt operierte. Um seine Marke zu stärken, tritt das Unternehmen mit seinen 80 Millionen Euro Jahresumsatz in Deutschland künftig unter dem Namen des Mutterunternehmens auf. Bisnode mit seiner Zentrale in Darmstadt ist mit dem bisherigen Geschäftsverlauf zufrieden. Datenschutzbedenken werden nicht gesehen. Bei jeder Anfrage müsse die KundIn ihr berechtigtes Interesse an der Anfrage nachweisen. Diese Angaben würden archiviert. Komme es zu rechtlichen Auseinandersetzungen, könne der Fall nachvollzogen werden. Plane eine PrivatkundIn z. B., einen Kaufvertrag mit einem Unternehmen zu schließen oder hat sie ein bestehendes Vertragsverhältnis, könne sie die Einzelauskunft anfordern, so ein Sprecher: „Wir halten es für sinnvoll, dass unser Angebot auch jemand nutzen kann, der keine dauerhafte Beziehung zu uns anstrebt, sondern sich vor einer großen Investition informieren will, die er nur einmal im Leben tätigt."

Die Auskunftei Schufa hat dasselbe Kundensegment im Blick. Vorstandsvorsitzender Michael Freytag erklärte, dass sich dort innerhalb von drei Jahren die Zahl der Privatkunden auf 1,6 Millionen verdoppelt habe. Bislang beschränkte sich die Dienstleistung darauf, für KundInnen nach Einträgen auf schlecht beleumundeten Internetseiten zu suchen. Nun will die Schufa ihre Datenbanken für Privatkunden öffnen und den Zugang über Smartphone-Apps erleichtern.

Creditreform, mit 15 Millionen Anfragen über Unternehmen bundesweit im Jahr führend und bei Anfragen über Privatpersonen hinter der Schufa die Nummer zwei, hält dagegen seine Datenbanken für private KundInnen verschlossen. Der Nachweis des vom Bundesdatenschutzgesetz (BDSG) geforderten berechtigten Interesse eines Auskunftwilligen ist bei PrivatkundInnen erheblich schwieriger. Es muss ausgeschlossen werden, dass jemand die finanzielle Situation des Nachbarn durchleuchtet und diese Informationen für private Zwecke missbraucht. Einige der 130 lokalen Vereine, aus denen Creditreform besteht, machen jedoch Ausnahmen. Ein Sprecher der Zentrale in Neuss erklärte für die Unternehmensgruppe mit einem Jahresumsatz von knapp einer halben Milliarde Euro, dass das Privatkundengeschäft nicht umsatzträchtig sei: „Wir versprechen uns von Privatkundenanfragen kein größeres Geschäft."

Der Berliner Wettbewerber Creditsafe erteilt bisher Auskünfte ausschließlich an Firmenkunden. Momentan seien die Kapazitäten des walisischen Unternehmens, so ein Sprecher, begrenzt; das Geschäftsmodell sei auf Abonnenten ausgerichtet. Um Einzelauskünfte zu ermöglichen, müsste die Infrastruktur teuer erweitert werden. Ebenso lehnt die Auskunftei Bürgel eine Öffnung ab. Mit 192 Millionen Euro Umsatz zählt sie zu den Großen der Branche. Bei Privatpersonen entstehe schnell eine rechtliche Grauzone,

so ein Unternehmenssprecher. Wenn aber eine Privatperson eine Information haben wolle, könne sie sich anders Zugang verschaffen: „Wer sich über ein Bauunternehmen informieren will, bekommt auch über einen Rechtsanwalt Auskunft, der mit uns in einer Geschäftsbeziehung steht." (Krohn, Bonitätsauskünfte für Privatkunden, www.faz.net 14.10.2013).

Bund/Länder

2012 neun „große Lauschangriffe"

Deutsche Strafverfolgungsbehörden haben im Jahr 2012 gemäß einer Unterrichtung durch die Bundesregierung an den Bundestag in neun Privatwohnungen Gespräche belauscht. Die Dauer der Überwachungen lag zwischen zwei und 61 Tagen. Die unter dem Namen ‚Großer Lauschangriff' bekannten Abhörmaßnahmen erfolgten im Rahmen von zwei Strafverfahren, die der Generalbundesanwalt führte, sowie sechs Verfahren in den Ländern Bremen, Hamburg, Niedersachsen und Nordrhein-Westfalen. Der ‚Große Lauschangriff' ist, nachdem das Bundesverfassungsgericht im Jahr 2004 frühere Regelungen verwarf, nur bei besonders schweren Straftaten zulässig. Dazu zählen Mord und Totschlag oder die Bildung einer terroristischen Vereinigung. Auch zur Gefahrenabwehr ist das Überwachen von Wohnungen möglich. Laut dem Bericht der Regierung ist dies aber im Jahr 2012 nicht erfolgt (Lauscher in Wohnungen, SZ 31.10.2013, 6).

Bund/USA

BfV, BND und CIA kooperierten bei „Projekt 6"

Im Rahmen der Snowden-Enthüllungen wurde das Undercover-"Projekt 6" oder „P6" bekannt, bei dem zwischen 2006 und 2010 ein Team aus Beamten des Bundesamtes für Verfassungsschutz (BfV), des Bundesnachrichtendienstes (BND) und der CIA (Central Intelligence Agency, US-Auslandsgeheimdienst) mit Hilfe einer neuen Software in einer Datenbank „PX" mehr über das Beziehungsgeflecht angeblicher Dschihadisten zu erfahren versuchten. Der grüne Bundestagsabgeordnete Konstantin von Notz fragte in knapp 50 Fragen im September 2013 bei der Bundesregierung nach den Hintergründen dieses Projektes. Die Antworten zu den Fragen 2 bis 42 wurden von der Regierung „aus Gründen des Staatswohls" als „Verschlusssache – Geheim" eingestuft. Eine Veröffentlichung von Einzelheiten würde „zu einer wesentlichen Schwächung" der Dienste bei der „Informationsgewinnung führen".

Auf Grund von Recherchen des NDR und der Süddeutsche Zeitung ist bekannt, dass die Initiative zur Gründung der Gruppe von der CIA ausging. Von Oktober 2006 an lief der Betrieb, erst in Neuss, dann von 2007 an wegen einer „Änderung der Sicherheitslage" in Köln. Ein CIA-Mann gehörte zu der Truppe. Das BfV stellte bis zu 9 Mitarbeitende ab, der BND erst einen, dann zwei. Die Leitung lag beim BfV. In Stellungnahmen der deutschen Dienste für die Regierung heißt es, die US-Agenten hätten „auf deutschem Boden keine Befugnisse zu Operationen gehabt". Ob sie sich hieran gehalten haben, wurde vom BfV und BND nicht bezweifelt. Der US-Kollege habe sich offiziell in Deutschland aufgehalten, schrieb das für Spionageabwehr zuständige BfV der Regierung. Die US-Amerikaner interessierten sich im Rahmen von „P6" für den NDR-Journalisten Stefan Buchen und forschten ihn aus. Buchen war der CIA offenkundig durch Telefonate mit Islamisten aus dem Jemen aufgefallen. Eine Sprecherin von Innenminister Hans-Peter Friedrich (CSU) hatte am 09.09.2013 erklärt, grundsätzlich könne „niemals ausgeschlossen werden", dass auch Informationen von Journalisten erfasst würden, wenn sie im terroristischen Umfeld recherchierten. Buchen forderte erfolglos Auskunft gemäß deutschem Datenschutzrecht. Die deutschen Dienste sagen, sie hätten bei der Journalistenrecherche nicht geholfen.

2010 erbat die CIA bei BND und BfV Informationen zu einer Person aus Deutschland, die einen „nicht identifizierten Gefährten" eines Qaida-Mitglieds angerufen haben solle. Allerdings könne man auf Basis „der gelieferten Adress- und Telefoninformationen" den namentlich genannten Anrufer nicht identifizieren. Nach Presserecherchen handelte es sich in diesem Fall bei dem Anrufer auf der angeblichen Dschihadisten-Nummer um einen Beamten aus Rheinland-Pfalz. Dieser hatte jedoch nicht mit einem Qaida-Aktivisten telefoniert, sondern mit seinem Schwager - damals Lehrer am Goethe-Institut des betroffenen Landes.

Die CIA nahm die für sie interessanten Daten mit, der Betrieb endete und die deutschen Dienste löschten die Datenbank. Deshalb könnten sie heute nicht mehr sagen, wen sie wann gespeichert hatten. Etwa 1119 Personen sollen es gewesen sein. Einen „echten Mehrwert für die Facharbeit" habe „P6" gemäß den Angaben der Dienste nicht gebracht. Auch diese Feststellung wurde in der Anfragenbeantwortung geheim gehalten. Mitglieder des Parlamentarischen Kontrollgremiums sowie der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit waren vom „Projekt 6" nicht in Kenntnis gesetzt worden (Goetz/Leyendecker, Hauptsache geheim, SZ 31.10.01.11.2013, 7; Gebauer/Medick, Geheime Einheit: „Projekt 6" bringt deutsche Nachrichtendienste in Erklärungsnot, www.spiegel.de 09.09.2013; Der Spiegel 39/2013, 22).

Niedersachsen

Verfassungsschutz speichert Daten von JournalistInnen

Thilo Weichert

Der Fall Röpke

Der Verfassungsschutz in Niedersachsen (VerfSch Nds.) hat in der Vergangenheit illegal JournalistInnen ins Visier genommen. Innenminister Boris Pistorius (SPD) teilte am 18.09.2013 in Hannover mit, dass mindestens 7 derartige Fälle in die Dateien des Verfassungsschutzes gelangten. Zulässig wäre eine Speicherung nur, wenn es Hinweise auf einen extremistischen Hintergrund gebe: „Es handelt sich um einen ernsten Vorgang. Die

Pressefreiheit ist ein hohes Gut, das vom Grundgesetz geschützt ist."

Eine der Betroffenen ist die Andrea Röpke. Auf Röpkes Anfrage hin habe der Verfassungsschutz 2012 mitgeteilt, dass keine Daten über sie gespeichert seien. Gegen den Vorgänger von Pistorius im Innenministeramt bis Februar 2013, Uwe Schünemann (CDU), wurden nun Bespitzelungsvorwürfe erhoben. Schünemann bewarb sich im Herbst 2013 erfolglos für den Landratsposten im Landkreis Hameln-Pyrmont. Die nach dem Regierungswechsel von CDU/FDP zu rot-grün ins Amt gekommene neue niedersächsische Verfassungsschutzpräsidentin Maren Brandenburger betonte, JournalistInnen seien vom Verfassungsschutz nicht abgehört und auch nicht observiert worden. Die Speicherungen der Behörde zu rund 9.000 Personen würden überprüft: „Ich gehe davon aus, dass es weitere Fälle geben wird." Sie sei auf die Fälle gestoßen, nachdem sie eine Prüfung der personenbezogenen Daten veranlasst hatte. Brandenburger löste den langjährigen Leiter Hans-Werner Wargel ab. Für ihn hatte sie zuvor die Öffentlichkeitsarbeit erledigt.

Der Fall der 48-jährigen Rechtsextremismus-Expertin und Autorin Andrea Röpke ist insofern speziell, dass diese sich im Februar 2012 beim Verfassungsschutz, nach gespeicherten Informationen über sich erkundigte. Im Antwortschreiben zwei Monate später betonte der VerfSch Nds., dass zu ihr „weder eine Akte geführt wird noch Angaben in Dateien gespeichert sind". Tatsächlich wurden die Einträge erst auf die Anfrage hin gelöscht. Brandenburger teilte Röpke nach Angaben ihres Anwalts am 18.09.2013 mit, dass über sie zwischen 2006 und 2012 Daten gesammelt worden seien. Röpkes Anwalt Sven Adam prüft nun eine verwaltungsgerichtliche Klage gegen die falsche Auskunft. Minister Pistorius wertete den Fall als bewusste Vertuschung. Der Anwalt von Röpke erklärte: „Zum Zeitpunkt der Anfrage wurde meine Mandantin noch überwacht." Offensichtlich sollte mit dem falschen Antwortschreiben „die sechsjährige rechtswidrige Überwachung vertuscht werden". Es werde nun um die vollständige Rekonstruktion der gesammelten Daten gehen. Röpke führt seit den 90er Jahren Recherchen über die rechtsextreme Szene durch. Neonazis veröffentlichten im Internet ihren Steckbrief. Bei einer Veranstaltung der neonazistischen „Heimattreuen Jugend" wurde sie mitten am Tag auf der Straße von rechtem Mob gejagt und geschlagen. In der Akte über Röpke sollen Veranstaltungen verzeichnet gewesen sein, auf denen Röpke aufgetreten ist. Vermerke sollen angelegt worden sein, weil auch LinksextremistInnen und Autonome zu den Zuhörenden gehört hätten. Sie ist für ihre Arbeit mehrfach ausgezeichnet worden, u. a. als „Journalistin des Jahres 2012" durch das Magazin „medium".

Weitere Betroffene

Neben Röpke sind von der Beobachtung bisher sechs weitere KollegInnen betroffen. Dies betrifft auch Personen, die nicht im rechten, sondern im linken Milieu recherchiert haben. Zu den Überwachten gehört auch der Berliner Journalist Ronny Blaschke, der sich durch Recherchen über rechtsextreme Umtriebe im Sport einen Namen gemacht hat. Er erhielt für seine Arbeit den angesehenen Julius-Hirsch-Preis. Dieser Preis wird seit einigen Jahren vom Deutschen Fußballbund (DFB) vergeben „für Menschenwürde und Toleranz, gegen Rassismus, Fremdenfeindlichkeit und Antisemitismus". Blaschke wurde u. a. angekreidet, dass er vor langer Zeit einen Gastvortrag bei der Partei Die Linke in Hannover gehalten hatte. Blaschke berichtet, dass er von einem Polizeibeamten wegen der „Diffamierung der Fußballvereine, vorwiegend der Fanszene in den neuen Bundesländern" angegriffen worden ist. Vor einem Vortrag in Thüringen hatte man ihn aufgefordert, die „Extremismusklausel" zu unterschrieben, damit der Veranstalter sicher gehen konnte, dass das Land nicht seine Förderung zurückzieht.

Zwei Jahre zuvor war der Fall des Journalisten und Redakteurs des Göttinger Stadtradios Kai Budler aufgeflogen, der auch über Neonazis berichtete. Der niedersächsische Verfassungsschutz, der im NSU-Fall nicht durch besondere Aufmerksamkeit auffiel, hatte ihn wohl als Linksextremist beobachtet und z. B. erfasst, dass er an „Anti-Atom-Demonstrationen" teilgenommen hat. Auch diese Akten wurden teilweise geschreddert, als der Anwalt Sven Adam nachhakte. Der VerfSch Nds. meinte Erkenntnisse zu haben, dass sich Budler „in extremistischen Personenzusammenhängen bewegt hat, und darum werden dann auch diese personenbezogenen Daten erhoben". Für Röpke war „auch der Fall Budler ein Grund, mal nachzufragen, ob es da was über mich gibt". Von den insgesamt sieben Personen wurden drei über die Erfassung unterrichtet. Zwei Journalisten sind nicht auffindbar, weil zu ihnen keine Kontaktdaten oder Wohnanschriften vorliegen. Die zwei weiteren Personen hatten schon Selbstauskünfte angefragt und daraufhin Auskunft erhalten.

Reaktionen

Der Präsident des VerfSch Nds. von 2007 bis 2009 und dann Nachrichtendienst-Koordinator im Bundeskanzleramt Günter Heiß wies eine Verantwortung für die rechtswidrige Speicherung von Daten über Journalisten zurück: „Ich habe von den Vorgängen keine Kenntnis." Dies liege auch daran, dass diese bereits lange her seien. Vor 2007 war Heiß für die Aufsicht über den Verfassungsschutz zuständig.

Kurz zuvor war in einem anderen Zusammenhang der Fall des NDR-Journalisten Stefan Buchen bekannt geworden. Der Reporter war im Jahr 2010 in den Fokus eines geheimen Datenprojekts zwischen dem Bundesamt für Verfassungsschutz (BfV), dem Bundesnachrichtendienst sowie der US-amerikanischen CIA geraten. Buchen war in US-Dokumenten mit seiner Pass- und Mobilfunknummer sowie seinem Geburtsdatum aufgetaucht. Über den deutschen Reporter wollten die US-Dienste gern mehr erfahren, nachdem er der CIA offenkundig durch Telefonate mit Islamisten aus dem Jemen aufgefallen war. Der Präsident des Bundesverfassungsschutzes, Hans-Georg Maaßen, bestritt, dass sein Amt Buchen beobachtet habe. Das BfV bewege sich stets „im Rahmen der gesetzlichen Regelungen", sagte er. „Dazu gehört, dass wir keine Journalisten beobachten" (s. o. S. 156: Bund/USA: BfV, BND und CIA kooperierten bei „Projekt 6").

Als Konsequenz aus den verbotenen Aktionen des VerfSch Nds. forderten SPD und Grüne eine Novelle des Verfassungsschutzgesetzes, so Klaus-Peter Bachmann (SPD) und Helge Limburg (Grüne): „Wir sind der Meinung, dass gespeicherte Daten vor ihrer Löschung den Betroffenen soweit möglich offengelegt werden müssen.“ Bislang schreibe das Gesetz die Löschung vor, bevor der Betroffene informiert wird. Limburg: „Davon haben die Betroffenen nichts, denn sie wissen nicht, was von ihnen gespeichert wurde.“ Auch der ehemalige Vorsitzende des NSU-Untersuchungsausschusses des Bundestages, Sebastian Edathy (SPD), kritisierte die Überwachung von JournalistInnen durch den Niedersächsischen Verfassungsschutz: „Es gibt erheblichen Aufklärungsbedarf – insbesondere hinsichtlich einer möglichen Mitwisserschaft des damaligen Innenministers Uwe Schünemann.“

Das Verhältnis Presse - Geheimdienste

Alle paar Jahre melden Medien, dass ein deutscher Geheimdienst JournalistInnen ausgespäht hat. Anschließend wird von den Behörden abgewiegelt, beteuert, erklärt, und es hagelt Versprechen: Ein bedauerlicher Einzelfall, einE MitarbeiterIn sei über die Stränge geschlagen oder habe sich irgendwie vertan.

Der frühere BND-Präsident Ernst Uhrlau hat nach einer Affäre des Auslandsgeheimdienstes gesagt: „Journalisten sind keine Fliegenfänger.“ An Treueschwüren („die Dienste arbeiten nach Recht und Gesetz“) ist bis zum nächsten Vorfall kein Mangel. Geheimdienste halten JournalistInnen nicht selten für Gegner oder für Gehilfen. Für beide Varianten gibt es Belege. Woher sie denn all ihre guten Informationen über Neonazis her habe, wurde Röpke von den Beamten des VerSch Nds. gefragt; sie sagte nichts. Das meiste von dem, was die Öffentlichkeit über eine neonazistische Gruppe wie die „Heimattreue Deutsche Jugend“ nach deren Verbot erfahren hat, verdankt sie nicht den Behörden, sondern der Arbeit von JournalistInnen wie Röpke, die von Geheimdiensten wenig hält.

Das Verhältnis zwischen Sicherheitsbehörden und Journalismus ist kompliziert. Die Medien möchten viel über die Arbeit der Dienste erfahren. Auch schmückt es, wenn in der Redaktion erzählt werden kann, eine Recherche stütze sich auf geheime Akten, auch wenn darin Unsinn steht. Dienstvorgesetzte möchten wissen, wo undichte Stellen in ihren Apparaten sind. Mitunter locken Dienste für hohe Preise JournalistInnen zum Mitmachen oder zum Verkauf ihres Wissens an. Schon vor Jahrzehnten hat der Deutsche Presserat darauf hingewiesen, es sei unzulässig, Aufträge von Geheimdiensten entgegenzunehmen.

Die Geheimdienste betrachten manche JournalistInnen als Schwestern und Brüder im Geiste, die sich auf das Geschäft mit Informationen verstehen. Das schmeichelt beiden Seiten. Vom Verfassungsschutz in Bayern verlautete: „Wir begrüßen es, wenn sich Journalisten tief in eine Materie hineinarbeiten.“ Dies sei eine „Ergänzung zu unserer Arbeit“. Das Amt versichert, auf keinen Fall würden Daten über JournalistInnen gespeichert, wenn sie wegen ihrer beruflichen Tätigkeit in Kontakt mit Extremisten kommen. In Niedersachsen sollen einige der betroffenen JournalistInnen in der DKP aktiv gewesen und deshalb ins Visier des Staates geraten sein.

Wird in den Behörden gegen Vorschriften verstoßen, kommt es meist erst nach einem Regierungswechsel heraus. Zu Beginn der sozialliberalen Koalition auf Bundesebene ließ sich der damalige Kanzleramtschef Horst Ehmke die Liste aller JournalistInnen geben, die mit den Geheimen unheimlich verbunden waren. Das Ergebnis: Erste Adressen des deutschen Journalismus standen auf der Gehaltsliste des BND. Ein Nahost-Experte sagte: „Schade, dass ihr so spät kommt. Ich liefere schon für die Franzosen“. Journalisten beteuern regelmäßig, nicht für die Geheimen zu arbeiten. Und die Geheimen erklären, sie verzichteten auf den Einsatz von JournalistInnen. Beides wird auch in Zukunft nicht zutreffen. 1988 sickerte durch, dass der VerfSch Nds. seinen Stab durch Journalisten ergänzt hatte. Ende 1993 versuchte der BND, den Mitarbeiter eines Hörfunksenders in Bonn anzuwerben. Eine Aufwandsentschädigung werde ihm garantiert. Zufällig hatte er sein Büro im selben Haus wie die Tageszeitung „taz“. Tiefen Einblick in die Szene brachten dann die Recherchen des ehemaligen Bundesrichters Gerhard Schäfer, der als Sonderermittler für den Bundestag im Jahr 2006 BND-Operationen analysiert hatte. Jahrelang hatte der BND willfährige JournalistInnen als Quellen geführt. Ihre Aufgabe war es unter anderem, Informationen über kritische KollegInnen zu sammeln. Schäfer ermittelte etwa ein halbes Dutzend ZuträgerInnen, die dem Dienst unheimlich behilflich waren. Besonders ein Journalist mit dem Decknamen „Sommer“ war in der Szene sehr aktiv.

Die Helfer bekamen für ihren Berufsverrat Geld oder Informationen – eine Win-Win-Situation, die für die Öffentlichkeit und das Publikum zugleich ein Totalverlust an Vertrauen darstellt. Nur wenige JournalistInnen beschäftigen sich intensiv mit den Geheimdiensten. Oft sind nur die Pressestelle und der jeweilige Präsident Anlaufstellen, die ihre Informationen loswerden wollen. Ob diese stimmen oder nicht, ist schwer überprüfbar. Vor vielen Jahren empfahl Eckart Spoo, der langjährige Vorsitzende der Deutschen Journalisten-Union: „Wir sollten allen Informationen aus Verfassungsschutzämtern prinzipiell den Glauben verweigern.“ Aus Sicht von Mitarbeitenden in den Sicherheitsbehörden ist die Verbindung von journalistischer Arbeit und einer Tätigkeit für einen Geheimdienst nichts Ehrenrühriges. Ein früherer BND-Präsident hat solche Kumpanei einmal als „patriotische Verhaltensweise“ gerühmt (Niedersachsen: Verfassungsschutz speichert Daten von Journalisten, www.spiegel.de 18.09.2013; Leyendecker/Schultz, Journalisten im Visier, SZ 19.09.2013, 29; Bewarder/Flade, Nachrichtendienst-Koordinator weiß von nichts, www.welt.de 20.09.2013; Leyendecker/Schultz, Totaler Vertrauensverlust, SZ 20.09.2013, 47; Leyendecker, Das ganze Ausmaß, SZ 25.09.2013, 31; Blaschke, Unter Verdacht, www.sueddeutsche.de 26.09.2013; vgl. DANA 4/2011, 177).

Schleswig-Holstein

Massenhaft polizeiliche Funkzellenabfragen

Gemäß einer Antwort der Landesregierung auf eine parlamentarische Anfrage der Fraktion der Piraten wurden seit 2009 bei polizeilichen Funkzellenabfragen in Schleswig-Holstein millionenfach Handys geortet. Ein Großteil der dabei gewonnenen Daten wurde dauerhaft gespeichert – in vielen Fällen auch, nachdem die jeweiligen Ermittlungsverfahren längst eingestellt waren. Bei Funkzellenabfragen werden sämtliche Telekommunikationsverbindungsdaten, die in einem zuvor festgelegten, räumlich abgegrenzten Bereich anfallen, erfasst. Voraussetzungen für diese Form der verdeckten Ermittlung sind eine richterliche Anordnung, die Verfolgung einer schweren Straftat und die Untauglichkeit weniger brachialer Ermittlungsmethoden.

Umfang und Erfolg der Maßnahmen in Schleswig-Holstein legen den Verdacht nahe, dass die Behörden dabei das richtige Maß verloren haben. Insgesamt 850 Abfragen wurden seit 2009 in die Wege geleitet, dabei nach Schätzungen der Piratenpartei bis zu sieben Millionen Handys geortet. Begründet wird die umfangreiche Erfassung mit dem Versuch von Polizei und Staatsanwaltschaft, die Verkehrsdaten verschiedener Tatorte und Tatzeiten auf Übereinstimmungen abzugleichen. Auf diese Weise sollten Straftatenserien aufgeklärt oder überhaupt als solche erkannt werden. Dies gelingt aber nur in den wenigsten Fällen: Gerade einmal 36 Verurteilungen sind unmittelbar auf die „nicht individualisierten Funkzellenabfragen“ zurückzuführen. In 111 Fällen brachten sie gemäß der Antwort neue Ermittlungsansätze. Die vier Staatsanwaltschaften in Schleswig-Holstein wenden das Instrument in höchst unterschiedlichem Ausmaß an. Im Raum Flensburg wurden gerade einmal 16 Abfragen initiiert, die Kieler Staatsanwaltschaft hingegen machte mit 336 Abfragen einundzwanzig Mal häufiger im gleichen Zeitraum Gebrauch von der Methode.

Die erhobenen Daten werden im Regelfall dauerhaft gespeichert: So wurden seit 2009 lediglich Datensätze aus 122 Vorgängen wieder gelöscht; 184 blieben bis zum Anfragezeitpunkt Mitte 2013 „in Bearbeitung“, auch bei Verfahren, bei denen die Ermittlungen schon lange abgeschlossen sind. Patrick Breyer, Mitglied der Piratenfraktion, sieht insbesondere in der langen Aufbewahrung der Verbindungsdaten einen klaren Rechtsbruch. Auch Barbara Körffer, die zuständige Referentin am Unabhängigen Landeszentrum für Datenschutz (ULD), hat mit der langen Speicherdauer Probleme. Sie kündigte die Überprüfung der Rechtmäßigkeit der Datenerhebung und der Verhältnismäßigkeit der weiteren Speicherung an. Geprüft werde auch, ob nicht viel mehr Besitzer polizeilich erfasster Handys über die Maßnahme informiert werden mussten. Das werde zwar bisweilen als weltfremd abgetan, so Marit Hansen, stellvertretende ULD-Chefin, „aber ich halte das überhaupt nicht für weltfremd“.

In der rot-grünen Regierungskoalition gibt es insofern unterschiedliche Sichtweisen. Grünen-Fraktionschefin Eka von Kalben zeigte sich vom Ausmaß des Datensammelns „überrascht“ und mahnte eine vernünftige „Balance“ zwischen Sicherheitsbedürfnissen und dem Recht auf Datenschutz an. Innenminister Andreas Breitner (SPD) erkannte dagegen keinen Handlungsbedarf. Die Abfragen seien von der Staatsanwaltschaft beantragt und gerichtlich genehmigt: „Mehr rechtsstaatliche Sicherung geht nicht“ (Harning, Big Brother in Schleswig-Holstein, www.neues-deutschland.de 19.08.2013).

Thüringen

Zahnarzt-Videospanner zu Haftstrafe verurteilt

Weil er seine Mitarbeiterinnen jahrelang heimlich in der Umkleide gefilmt hat, wurde ein Geraer Zahnarzt am 27.09.2013 vom Amtsgericht Gera wegen 211 Fällen zu zwei Jahren und vier Monaten Haft verurteilt. Richter Siegfried Christ begründete sein Urteil: „Das Auge eines anderen hat in der Umkleide nichts zu suchen.“ Der heute 52-Jährige sei ziemlich skrupellos vorgegangen, ohne jedes Mitgefühl für die Opfer. Auch im Prozess sei kein Wort der Entschuldigung über seine Lippen gekommen. Ermittler hatten auf Datenträgern des Zahnarztes knapp 7500 Dateien aus den heimlichen Videoaufnahmen gefunden oder wiederherstellen können. Den Angaben nach sind die Frauen in den Videoaufnahmen in Unterwäsche oder nackt zu sehen. Die Anklage hatte drei Jahre Haft gefordert, die Verteidigung einen Freispruch. Das Urteil ist noch nicht rechtskräftig (Zahnarzt filmt heimlich Frauen – Haftstrafe, SZ 28./29.09.2013, 11; Frauen heimlich gefilmt: Haftstrafe für Spanner-Zahnarzt, www.focus.de 27.09.2013).

Datenschutznachrichten aus dem Ausland

Europa

Datenschutz beim Kampf gegen Menschenhandel

Vom 25. bis 27.09.2013 fand in Berlin eine Konferenz zum Thema „Datenschutz und informationelle Selbstbestimmung für marginalisierte Gruppen: eine neue Herausforderung in der Politik zur Bekämpfung des Menschenhandels“ statt. Dabei wurde erstmals die Sammlung, Verarbeitung sowie Weitergabe personenbezogener Daten von Betroffenen im Kampf gegen Menschenhandel öffentlich diskutiert. Hintergrund für diese Erörterung ist, dass die Datenerhebung und -verarbeitung zu Opfern des Menschenhandels für diese schwerwiegende Konsequenzen haben kann, etwa die langfristige soziale Stigmatisierung oder die erneute Bedrohung durch die TäterInnen. Bisher ist der Datenschutz ein noch wenig bekanntes auch nicht verbindlich gestaltetes Thema. Die Folge ist das Fehlen von Orientierungshilfen z. B. für die MitarbeiterInnen von Beratungsorganisationen. Auf der europäischen datACT-Konferenz trafen sich Interessierte aus Nichtregierungsorganisationen, Regierungen, internationalen Organisationen und Wissenschaft aus 15 europäischen Ländern in Berlin. Unter Mitwirkung der UN-Sonderberichterstatterin für zeitgenössische Formen der Sklaverei, Gulnara Shahinian, brachte die Konferenz erstmals Sachverständige aus dem Datenschutz und AkteurInnen aus der Menschenhandelsbekämpfung zusammen.

Der schleswig-holsteinische Datenschutzbeauftragte Thilo Weichert meinte in seinem Eingangsstatement: „Die informationelle Selbstbestimmung für Betroffene von Menschenhandel und anderen marginalisierten Gruppen ist regelmäßig nicht existent. Daran ändert sich wenig, wenn sie aus den Fängen der Menschenhändler und Schleuserorganisationen entkommen. Sie unterliegen dann einer staatlichen oder halbstaatlichen Fürsorge und Aufsicht, die mit einer umfassenden informationellen Kontrolle einhergeht. Diese dient einerseits – fürsorgend – der Betreuung der Betroffenen. Sie dient zugleich aber auch deren Freiheitsbegrenzung.“ Während Deutschland noch vor der Einrichtung einer nationalen Berichterstattungsstelle oder äquivalenter Mechanismen steht, sind zahlreiche EU Länder der Forderung der im Jahr 2011 verabschiedeten EU-Richtlinie 2011/36/EU „Zur Verhütung und Bekämpfung des Menschenhandels und zum Schutz seiner Opfer sowie zur Ersetzung des Rahmenbeschlusses 2002/629/JI des Rates“ nachgekommen. Aktuell existieren in Europa verschiedene Formen von Datensammlungs- und Datenauswertungsinitiativen und verschiedene Kooperationsmodelle zwischen Behörden und Nichtregierungsorganisationen. Es gibt allerdings Bestrebungen, diese Berichterstattungsstellen in den kommenden Jahren EU-weit zu vereinheitlichen. Deshalb sind nach Ansicht der Teilnehmenden der Konferenz klar festgelegte Inhalte und Verfahren bei der Kooperation zwischen Datensammlungsbehörden und zivilgesellschaftlichen AkteurInnen nötig, wobei die Verantwortlichkeiten und Mandate der jeweiligen InteressenvertreterInnen klar voneinander abzugrenzen sind. Die Teilnehmenden stellten fest, dass Daten niemals machtneutral und unschuldig sind. Vielmehr käme ihnen ein kommerzieller Wert zu. Ihnen sei je nach Interpretation auch die Gefahr immanent, sich gegen die Interessen und den Schutz der Betroffenen von Menschenhandel zu richten.

Die Konferenz gab Einblick in Möglichkeiten, wie Daten für und von Betroffenen zur Stärkung ihrer Rechte genutzt werden können. Bärbel Heide Uhl, Koordinatorin des datACT-Projektes erklärte: „Freiheit, nicht Angst, sollte die Prämisse aller rechtsbasierten Maßnahmen gegen Menschenhandel sein. Wir können als europäische anti-trafficking-community uns von dem Slogan ‚Freiheit statt Angst' der DatenschutzaktivistInnen inspirieren lassen.“ Das Projekt datACT wurde vom KOK e.V – Bundesweiter Koordinierungskreis gegen Frauenhandel und Gewalt an Frauen im Migrationsprozess in Zusammenarbeit mit dem europäischen Netzwerk gegen Menschenhandel La Strada International initiiert, um das Recht von Betroffenen des Menschenhandels auf Privatsphäre, Autonomie und Schutz der persönlichen Daten in Deutschland und anderen europäischen Ländern zu stärken (KOK-PE 01.10.2013, www.datact-project.org; Kontakt: KOK – Bundesweiter Koordinierungskreis gegen Frauenhandel und Gewalt an Frauen im Migrationsprozess e.V. Kurfürstenstr. 33 10785 Berlin Tel.: 030 / 26 39 11 93 Fax: 030 / 26 39 11 86; E-Mail : info@kok-buero.de; vgl. auch www.datenschutzzentrum.de/vortraege/20130925-weichert-datenschutz-menschenhandel.html).

Frankreich

Videoüberwachung unter Beobachtung

In Frankreich gibt es relativ wenig Widerstand gegen die auch dort zunehmende Videoüberwachung. Es gibt dagegen kaum Veranstaltungen oder Demonstrationen. Philippe Boulland, Mitglied der konservativen UMP, ist insofern eine Ausnahme: „Diese automatisierte Überwachung verbunden mit der Sammlung von persönlichen Informationen stellt eine Bedrohung für die persönliche Freiheit dar.“ AktivistInnen haben nun eine frankreichweite Überwachungskarte mit dem Namen „Sous surveillance“ (deutsch: „Unter Überwachung“) als Projekt gestartet, wo jedeR Standorte von Videokameras eintragen kann. 22 Städte und mehr als 7.000 Kameras hat die Website bereits verzeichnet. Dabei wird nicht nur der Standort angezeigt,

sondern auch versucht abzuschätzen, wohin die Kameralinse gerichtet ist und was sie sehen kann. Jérôme Leignadier-Paradon, Chef der Lyoner Piratenpartei, ist Entwickler der Karte. Die meisten Menschen würden die Kameras gar nicht mehr bemerken, das solle mit dem Angebot anders werden. Man wolle die Menschen auf Kameras hinweisen: „Die Gesichtsidentifikation von Facebook kombiniert mit der Geolokalisierung von GoogleMaps sind bereits Realität." Das FBI arbeite an entsprechenden Verfahren. Für ihn stellt die Technik daher die Frage, ob die Gesellschaft das Recht auf Privatsphäre aufrechterhalten wolle: „Freie Betriebsratswahlen oder das Demonstrationsrecht könnten so gefährdet werden." Und nun weitet sich das französische Projekt auch nach Deutschland aus. Vergleichbare Pläne gibt es in Deutschland für Hannover; für Bayern gibt es bereits eine Karte, in der schon 17.000 Kameras verzeichnet sind (Schmidt, Wo die Kameras stehen und hängen, www.zeit.de 19.08.2013; Vollmer, Mehr Bewusstsein für die Videoüberwachung, www.datenschutz.de 20.08.2013; http://www.sous-surveillance.net/;).

USA

Anonymes Surfen nach Snowden-Ermittlungen abgestellt

Das US-Unternehmen CryptoSeal hat seinen Service zum anonymen Surfen im Internet für private KundInnen abgeschaltet. Die Firma erklärte, nach derzeitigem US-Recht könne sie die versprochene Anonymität nicht mehr sicherstellen. Mit CryptoSeal Privacy wurde den Nutzenden ein anonymisierter Netzzugang angeboten. Die digitale Tarnkappe verschleiert den Datenverkehr mittels Durchleitung durch mehrere Server.

Aus dem Vorfall um den E-Mail-Dienstleister Lavabit habe man gelernt, dass die Regierung den Standpunkt vertrete, Internetdienstleister könnten jederzeit die Herausgabe der SSL-Schlüssel erzwingen. Das FBI hatte mit Geheimbeschlüssen Zugriff auf Nutzerdaten des auch von Edward Snowden genutzten verschlüsselten E-Mail-Service Lavabit gefordert. Daraufhin hatte Lavabit-Gründer Ladar Levison den Service im September unter massivem Protest geschlossen und juristische Schritte gegen die Geheimanordnungen eingeleitet. Das CryptoSeal-System sieht die Aufzeichnung entsprechender Daten nicht vor; es sei technisch auch nicht möglich, eine derartige Funktion kurzfristig bereitzustellen. Nach Ansicht des Unternehmens verstoßen derartige Anfragen gegen die US-Verfassung. Bis zu einer endgültigen Klärung der Angelegenheit könne der Service nicht weiter angeboten werden.

CryptoSeals Business-Sparte „Connect" ist von der Maßnahme nicht betroffen, weil sie nicht wie BitTorrent oder andere Filesharing-Dienste konstruiert sei und auch nicht das Ziel der Anonymität gegenüber dem Rechtssystem verfolgt. Interessierte User werden an alternative Dienste wie das Tor-Projekt verwiesen. CryptoSeal-Chef Ryan Lackey erklärte, er habe vor allem die finanziellen Risiken gescheut, die mit einer juristischen Auseinandersetzung mit US-Behörden verbunden seien. Unterm Strich seien einschlägige Dienste, die außerhalb der USA von Nicht-US-BürgerInnen betrieben würden, die bessere Option. Es gebe keinen Grund, einen privaten VPN-Dienst in den USA anzubieten und dabei Gefahr zu laufen, auf Behördenanordnung seine KundInnen „zu bescheißen" (US-Firma stellt Angebot zum anonymen Surfen ein, www.spiegel.de 23.10.2013).

USA

Kalifornien will Kinder vor Paparazzi schützen

Im kalifornischen Parlament wird der Gesetzentwurf SB606 diskutiert, wonach Kinder berühmter Menschen vor zudringlichen Kameras geschützt werden sollen. Vor dem Justizausschuss des Parlaments setzten sich in Sacramento u. a. die Schauspielerinnen Halle Berry und Jennifer Garner für den Entwurf ein. Berry berichtete, dass ihre fünfjährige Tochter sie einmal unter Tränen gefragt habe, ob die Männer sie töten wollten, die sie da draußen mit ihren Fotoapparaten bedrängt hatten. Garner, Mutter von drei Kindern, erzählte von unerträglichen Attacken durch Klatschreporter. Das geplante Gesetz sieht vor, dass Erziehungsberechtigte ihr Einverständnis zum Abdruck von Kinderfotos geben müssen (Mütter gegen Paparazzi, Der Spiegel 34/2013; Schwartz, Jennifer Garner, Halle Berry testify for stricter anti-paparazzi laws, blog.zap2it.com, 14.08.2013).

USA

Kalifornisches „Radiergummi-Gesetz"

Im US-Bundesstaat Kalifornien wurde ein Gesetz verabschiedet, das vorsieht, dass jedeR Nutzende eines sozialen Netzwerkes das Recht erhält, von ihm eingestellte Fotos, Filme oder Texte bis zu seinem 18. Geburtstag wieder entfernen zu können. Damit soll verhindert werden, dass sich Jugendliche mit kompromittierenden Bildern oder sonstigen Angaben oder Einträgen, die noch jahrelang im Netz zu finden sind, später um Berufschancen bringen. Die Regelung soll zum 01.01.2015 in Kraft treten. KritikerInnen halten die Regelung für wirkungslos, weil besonders kompromittierende Bilder oft im Netz kopiert und weitergegeben werden, so dass sie ein unkontrollierbares Eigenleben führen. Zudem erfasst das „Radiergummi-Gesetz" nur selbst eingestellte Inhalte, nicht die der durch Freunde oder – was manchmal noch heikler ist – die durch Exfreunde eingestellten Bilder und Einträge. Zudem rennt das Gesetz teilweise offene Türen ein, zumal soziale Netzwerke wie z. B. Facebook oder Twitter ihren Nutzenden längst gestatten, alte Beiträge vom eigenen Profil wieder zu entfernen (Der Spiegel 41/2013, 139).

Russland

Totalüberwachung von Olympia in Sotschi geplant

Der russische Inlandsgeheimdienst FSB will SportlerInnen und BesucherInnen der Olympischen Winter-

spiele im Februar 2014 in Sotschi umfassend ausspähen können. Die Behörde will die Kommunikation per Telefon, Smartphone und Internet vollständig überwachen, jedes Telefonat und jeden Datenverkehr. E-Mails, Webchats und Unterhaltungen über soziale Medien sollen nach Schlagworten und ganzen Suchphrasen durchkämmt werden können. Eingesetzt werden soll dazu auch die sogenannte Deep Packet Inspection, eine Technik zum Durchleuchten einzelner Datenpakete.

Die Überwachung in Sotschi ist kein punktueller Einsatz von Spähtechnik in Russland, sondern steht im Zusammenhang mit einem landesweiten System namens Sorm. Das Kürzel steht für „System für operative Ermittlungsaktionen". Sorm wird vom russischen Staat dazu benutzt, Telefonate und Internetkommunikation abzuhören. Aktuell wird die Sorm-Infrastruktur russlandweit modernisiert, ein besonderer Schwerpunkt liege auf Sotschi. Dort wird für die Olympischen Spiele durch Rostelecom ein leistungsfähiges LTE-Hochgeschwindigkeitsnetzwerk hochgezogen, das die BesucherInnen der Sportveranstaltung kostenlos benutzen dürften. Parallel soll im Geheimen ein System der Überwachung mitwachsen. Eine noch nicht unterzeichnete Anordnung vom März 2013 legt fest, dass Sorm dazu befähigt sein soll, auch Dienste aus dem Westen, namentlich Gmail und Yahoo, zu überwachen.

Grundlage für die Spähmaßnahmen sind die russischen Gesetze zur Fernmeldeüberwachung. Sie besagen unter anderem, dass alle Telefonanbieter und Internetprovider sogenannte Sorm-Boxen in ihre Hardware einbauen müssen. Über die Boxen kann der FSB Daten abrufen, ohne dass der Provider darüber Bescheid weiß. So lassen sich alle Telefonate und die Internetkommunikation abhören, ohne dass der FSB Rechenschaft ablegen muss. Die russischen InvestigativjournalistInnen Andrei Soldatow, Autor eines Buches über die Geschichte des russischen Geheimdienstes seit dem Ende der Sowjetunion, und Irina Borogan haben die Geschichte zusammen mit Shaun Walker für die britische Zeitung „Guardian" recherchiert. Sie schreiben, dass der FSB seit 2010 daran arbeite, Sorm für die Winterspiele 2014 einsatzbereit zu machen. „Die russischen Behörden wollen sicherstellen, dass jede Verbindung und jeder Schritt, den jemand von Sotschi aus während der Spiele im Netz macht, absolut transparent ist für die Geheimdienste des Landes." Ergänzend zur Netzüberwachung will Russland 5.000 Überwachungskameras in der Stadt am Schwarzen Meer installieren und 40.000 Polizisten einsetzen. Außerdem hat der Geheimdienst zwei Sonarsysteme gekauft, um U-Boote aufspüren zu können und gegen eine Attacke vom Wasser aus gewappnet zu sein. Die Oberaufsicht über die Operation wurde Oleg Syromolotow übertragen, einem langjährigen Leiter der Spionageabwehr. Soldatow: „Alles in allem sieht es danach aus, als würden diese Leute nach wie vor die größte Bedrohung für die Olympischen Spiele nicht aus dem Nordkaukasus erwarten, sondern aus dem Ausland." Der Geheimdienst ist auch schon beim Weg des Olympischen Feuers präsent: Als die Fackel plötzlich erlosch, war es ein Sicherheitsmann, der sie mit seinem Feuerzeug wieder ansteckte, was zu Scherzen beitrug: „Jetzt wird das Feuer des Geheimdienstes nach Sotschi getragen."

Das US-Außenministerium warnte alle AmerikanerInnen, die die Winterspiele in Sotschi besuchen wollen, vor der Überwachung. Am besten sollten sie elektronische Geräte, die nicht unbedingt gebraucht werden, zu Hause lassen. Wo das nicht möglich sei, sollten „alle persönlichen Daten und sensiblen Informationen entfernt werden". Reisende sollten außerdem darauf verzichten, sich über örtliche Internetanbieter in Cafés, Hotels oder Flughäfen einzuwählen. Der drahtlose Datenempfang sollte möglichst ganz abgeschaltet werden: „Ändern Sie alle Passwörter vor und nach der Reise."

Ron Deibert, Professor an der Universität von Toronto und Direktor des dort angesiedelten Citizen Lab, einer interdisziplinären Forschungseinrichtung zu Informations- und Kommunikationstechnik, verglich: „Sogar während der Olympischen Spiele in Peking gab es keine so ausgefeilte Überwachung und keine solchen Verfolgungsmöglichkeiten, wie sie heute existieren." Er spekuliert, dass Russland die Technik auch gegenüber homosexuellen Athleten verwenden könnte. Ein Mitarbeiter des russischen Geheimdienstes, Alexej Lawrischtschew, hatte sich vor wenigen Tagen noch abfällig über die Sicherheitsmaßnahmen für die Olympischen Spiele in London geäußert und eine Atmosphäre der Überwachung moniert. „Die Straßen und öffentlichen Plätze waren vollgestopft mit Überwachungskameras, sogar – entschuldigen Sie mich – in den Toilettenhäuschen." Russland werde so etwas nicht tun. Damit meinte er offenbar nicht, dass Russland die Spiele nicht überwachen will, sondern, dass man die SportlerInnen und BesucherInnen aus der ganzen Welt lieber im Unklaren darüber lässt, dass man sie ausspioniert (Gruber, Russland will vollständige Netzüberwachung bei Olympia, www.zeit.de 07.10.2013; Hans, Moskaus Agenten überwachen Olympia, SZ 08.10.2013, 1, 4).

Iran

Soziale Netzwerke vor Freigabe

Das iranische Telekommunikationsministerium teilte am 08.10.2013 mit, dass erwogen wird, den freien Zugang zu den sozialen Netzwerken Facebook und Twitter wieder zu eröffnen. Arbeitsgruppen aus verschiedenen Behörden seien dabei, die Aufhebung der Blockade der beiden Netzwerke zu überprüfen. Obwohl bisher die Nutzung von Facebook und Twitter in Iran verboten war, wird geschätzt, dass mehr als 20 Mio. IranerInnen Mitglied dieser Netzwerke sind (Facebook für Iraner, SZ 09.10.2013, 19).

Technik-Nachrichten

Automatisierter Kommunikationstrainer

Am Massachusetts Institute of Technology (MIT) wird eine sog. MACH-Software entwickelt, mit der Menschen ihre „sozialen Fertigkeiten“ verbessern können sollen, um z. B. bei Bewerbungsgesprächen einen besseren Eindruck zu hinterlassen. Ein Avatar steht zum Gespräch bereit, stellt Fragen, gibt kurze Antworten und nickt verständnisvoll. Unterdessen nimmt eine Webcam die KandidatIn auf. Ein Computerprogramm analysiert anschließend Mimik, Sprache und Gesprächsverhalten und liefert einen detaillierten Report. So wird der ProbandIn z. B. rückgekoppelt, ob sie häufig Füllwörter wie „ähm“ benutzt, wie viele Pausen sie macht, ob sie lächelt und wie sie die Sprache moduliert. Der Entwickler des Systems, MIT-Doktorand Ehsan Hoque, erläutert: „Sozialkompetenz ist der Schlüssel zum persönlichen und beruflichen Erfolg.“ Mit der Erfindung könne man jederzeit und unbeobachtet trainieren. Hoque berichtet, dass vom Avatar trainierte ProbandInnen sich eloquenter und kommunikativer präsentierten. Die „brutale Wahrheit“ über die eigenen Unzulänglichkeiten sei einfacher zu akzeptieren, wenn sie von einem Rechner komme (Der Spiegel 36/2013, 112).

Rechtsprechung

EGMR

Serbischer Geheimdienst muss Überwachtenzahlen offenlegen

In einer Kammerentscheidung urteilte der Europäische Gerichtshof für Menschenrechte (EGMR) in Straßburg am 26.06.2013, dass der Serbische Geheimdienst verpflichtet ist, der Nichtregierungsorganisation „Jugendinitiative für Menschenrechte“ mitzuteilen, wie viele Menschen im Jahr 2005 von der elektronischen Überwachung des Dienstes betroffen waren (Youth Initiative for Human Rights v. Serbia, app. no. 48135/06). Die Auskunftsverweigerung des Dienstes stelle einen Verstoß gegen die Meinungsfreiheit dar, die in Art. 10 der Europäischen Konvention für Menschenrechte (EMRK) gewährleistet wird. Zugleich sei damit gegen nationales Recht sowie gegen das Willkürverbot verstoßen worden.

Die 2003 gegründete Jugendinitiative mit Sitz in Belgrad hat sich zur Aufgabe gemacht, die Umsetzung von Übergangsgesetzen unter den Aspekten Menschenrechte, Demokratie und Rechtsstaatlichkeit zu beobachten. Sie forderte unter Berufung auf das nationale Informationsfreiheitsgesetz den Serbischen Geheimdienst auf, mitzuteilen, wie viele Menschen dieser im Jahr 2005 elektronisch überwacht hat. Der Dienst verweigerte dies mit dem Argument, diese Informationen seien geheim. Daraufhin beschwerte sich die Initiative beim Serbischen Informationsfreiheitsbeauftragten, dessen Aufgabe es ist, die Einhaltung des Informationsfreiheitsgesetzes aus dem Jahr 2004 zu kontrollieren. Dieser entschied im Dezember 2005, dass die Auskunftsverweigerung unzulässig sei und ordnete an, die geforderte Information innerhalb von drei Tagen zur Verfügung zu stellen. Eine Klage hiergegen wurde vom obersten Gerichtshof im April 2006 zurückgewiesen. Im September 2008 teilte der Geheimdienst der Jugendinitiative mit, die geforderten Informationen seien gar nicht vorhanden.

Die mit sieben RichterInnen besetzte Kammer des EGMR stellte fest, dass der geltend gemachte Auskunftsanspruch im öffentlichen Interesse lag, da die Information in die öffentliche Debatte eingebracht werden sollte. Die Weigerung mitzuteilen, wie viele Menschen elektronisch vom Dienst überwacht werden, verstieß gegen das Recht auf Meinungsäußerung der Antrag stellenden Nichtregierungsorganisation. Das nationale Recht sieht vor, dass diese Information auf Antrag offengelegt werden muss, was auch von der zuständigen Behörde bestätigt worden ist. Die letztlich vorgetragene Behauptung, die geforderte Information sei überhaupt nicht verfügbar, sei unglaubwürdig angesichts des Charakters der geforderten Daten und der ursprünglichen Verweigerung aus Geheimhaltungsgründen. Die Verweigerung war demgemäß willkürlich und ein Verstoß gegen Art. 10 EMRK. Angesichts des Umstandes, dass alternative Möglichkeiten zur Beantwortung der einfachen Fragestellung nicht bestanden, wurde der Geheimdienst direkt zur Angabe der Information verurteilt. Serbien kann diese Entscheidung noch vor der großen Kammer des EGMR anfechten (Press Release European Court of Human Rights, ECHR 186(2013) vom 25.06.2013; Voorhoof, inforrm.wordpress.com 09.07.2013).

EuGH

Aufnahme in Terrorliste ist begründungspflichtig

Die Europäische Union (EU) darf gemäß einem Urteil des Europäischen Gerichtshofes (EuGH) vom 18.07.2013 das Vermögen des in Saudi-Arabien lebenden Yassin Abdullah Kadi nicht einfrieren (C-415/05P). Die UN hatte den Mann 2001 auf eine Terrorliste gesetzt. Der EuGH meinte, es sei nicht ausreichend bewiesen, dass er tatsächlich in terroristische Aktivitäten verstrickt ist. Die Luxemburger Richter bestätigten damit ihre Rechtsprechung, dass die Aufnahme in eine Terrorliste gerichtlich voll überprüfbar ist.

Eine Reihe von Resolutionen des Sicherheitsrats verpflichtet alle UN-Mitgliedstaaten, Gelder und andere finanzielle Vermögenswerte von Personen oder Organisationen, die mit Osama bin Laden, Al-Qaida oder den Taliban in Verbindung stehen, einzufrieren. Zwecks Umsetzung dieser Resolutionen führt die EU eine Terrorliste mit den Namen der betreffenden Personen, die regelmäßig an eine entsprechende Liste der UN angepasst wird. 2008 stellte der EuGH mit dem Urteil „Kadi I“ fest, dass die Handlungen der EU grundsätzlich umfassender gerichtlicher Kontrolle unterliegen, auch wenn es um die Umsetzung von UN-Resolutionen geht. 2005 hatte das Gericht die Terrorliste noch für nicht überprüfbar gehalten. Die Verordnung, mit welcher der Name von Kadi in die Terrorliste aufgenommen worden war, wurde für nichtig erklärt, weil sie gegen die Verteidigungsrechte und das Recht auf effektiven gerichtlichen Rechtsschutz verstoße. Dem Mann waren nämlich keine der ihm zur Last gelegten Umstände, nicht einmal die Gründe für seine Aufnahme in die Liste, mitgeteilt worden. Daraufhin übersandte die EU-Kommission Kadi die ihr von der UN übermittelte Begründung für seine Aufnahme in die Liste und gab ihm Gelegenheit zur Stellungnahme. Kadis Name blieb anschließend aufgrund einer neuen Verordnung auf der Terrorliste. Dagegen wehrte sich der Mann erneut gerichtlich, womit er bereits in der ersten Instanz Erfolg hatte. Das Gericht der Europäischen Union erklärte auch die neue Verordnung für nichtig. Die Begründung der UN für die Aufnahme Kadis auf die Terrorliste erschien den Richtern insgesamt zu vage.

Die Anfechtung dieser Entscheidung vor dem EuGH durch die Kommission, den Rat und Großbritannien blieb erfolglos. Dem Betroffenen müsse mitgeteilt werden, warum sein Name auf eine Terrorliste gesetzt wird. Zwar sei der überwiegende Teil der Gründe, die gegen Kadi vorliegen, hinreichend präzise und konkret, um eine sachdienliche Ausübung der Verteidigungsrechte und eine gerichtliche Kontrolle der Rechtmäßigkeit der Aufnahme in die Terrorliste zu ermöglichen. Allerdings sei nicht bewiesen worden, dass Kadi in den internationalen Terrorismus verwickelt sei. Er selbst hatte dies stets entschieden zurückgewiesen. Die EU darf seinen Namen mithin nicht auf der Terrorliste belassen. Der EuGH bestätigte mit seinem Urteil, dass die EU Personen, die sie auf eine Terrorliste setzt, zumindest die Begründung der UN dafür übermitteln muss. Zudem müsse die EU dem Betroffenen ermöglichen, zu den Vorwürfen Stellung zu nehmen. Auf dieser Grundlage müsse die EU anschließend eigenständig prüfen, ob der Name zu Recht auf eine Terrorliste gesetzt werden darf. Es sei nicht Sache des Betroffenen, den negativen Beweis zu erbringen, dass die Begründung der UN nicht stichhaltig ist (EU darf Kadis Gelder nicht einfrieren, www.lto.de 19.07.2013; Janisch, Dünne Beweislage, SZ 19.07.2013, 8).

EuGH

Fingerabdruck auf EU-Reisepass rechtens

Der Europäische Gerichtshof (EuGH) urteilte am 17.10.2013, dass bei Antrag auf Ausstellung eines Reisepasses in der Europäischen Union (EU) die Pflicht besteht, Fingerabdrücke abzugeben (C-291/12). Der Anwalt Michael Schwartz aus Bochum war mit seiner Klage gegen die entsprechende EU-Verordnung aus dem Jahr 2004 erfolglos. Das Verwaltungsgericht (VG) Gelsenkirchen hatte die Klage von Schwartz dem EuGH vorgelegt. Zwar stellt, so der EuGH, die Erfassung und Speicherung von Fingerabdrücken im Reisepass einen Eingriff in die Rechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten dar, doch sei das gerechtfertigt, „um die betrügerische Verwendung von Reisepässen zu verhindern“. Mit den Fingerabdrücken werde das „dem Gemeinwohl“ dienende Ziel verfolgt, „die illegale Einreise von Personen in die Europäische Union zu verhindern“.

Der Kläger hatte argumentiert, die entsprechende EU-Verordnung verstoße ohne Not gegen den Datenschutz und gegen sein Recht auf Privatsphäre. Reisepässe seien auch ohne Fingerabdrücke in hohem Maß fälschungssicher. In Deutschland beispielsweise seien kaum Fälle bekannt, bei denen komplette Pässe gefälscht wurden. Zugleich habe der Chaos Computer Club bereits mehrfach gezeigt, wie leicht sich Fingerabdruckscanner täuschen und Fingerabdrücke fälschen lassen. Fingerabdrücke würden am Problem der illegalen Einwanderung nicht das Geringste ändern. Die meisten Menschen, die illegal in die EU einreisen, kämen nicht mit einem gefälschten Reisepass in der Hand. Entweder haben sie einen gültigen Pass und ein gültiges Visum und bleiben länger als sie dürften, oder sie kommen ganz ohne Ausweispapiere.

Der EuGH meinte hingegen, „der Wesensgehalt der fraglichen Grundrechte“ werde geachtet. Das Argument des Klägers, das System sei fehleranfällig, wies das Gericht unter Hinweis auf den hohen technischen Sicherheitsstandard zurück. Die Sorge, der digitalisierte Fingerabdruck könne leicht in einer Zentraldatei landen, versuchte es durch Hinweis auf die einschlägige EU-Verordnung zu zerstreuen, die „als solche keine Rechtsgrundlage für eine etwaige Zentralisierung der auf ihrer Grundlage erfassten Daten“ darstelle. Die Fingerabdrücke würden die Gefahr erheblich vermindern, „dass unbefugte Personen fälschlich zur Einreise in das Unionsgebiet zugelassen werden“. Rechtsanwalt Schwartz hatte die Iris-Erkennung als weniger riskant bewertet. Der EuGH meinte dagegen, dass diese Methode „unstreitig technisch noch

nicht so ausgereift wie die Erfassung von Fingerabdrücken" sei. Außerdem sei dieses Verfahren „gegenwärtig deutlich kostspieliger".

Der parteilose Bundestagsabgeordnete und frühere Richter Wolfgang Nešković hatte den Kläger in der mündlichen Verhandlung vor dem EuGH vertreten. Er erklärte zu dem Urteil, die europäischen Grundrechte befänden sich bei diesem Gericht offensichtlich „nicht in guten Händen". Im Zweifel müsse die Freiheit Vorrang haben, nicht die Sicherheit: „Für einen Gerichtshof, der sein juristisches Grundverständnis in der Welt der Kapital- und Dienstleistungsfreiheit entwickelt hat, stellt es eine große Herausforderung dar, den individuellen Grundrechten im Zweifel den Vorrang gegenüber den vorgegeben Sicherheitsinteressen der staatlichen Behörden einzuräumen" (Biermann, EuGH hält Fingerabdrücke im Pass für rechtens, www.zeit.de 17.10.2013: Janisch, Ärgerlicher Richterspruch zum Fingerabdruck, www.sueddeutsche.de 17.10.2013; Janisch, Pflicht zum Fingerabdruck, SZ 18.10.2013, 6).

BVerfG

Versicherer erneut beim Beschaffen von Gesundheitsdaten gebremst

Gemäß einem Beschluss der 3. Kammer des 1. Senats des Bundesverfassungsgerichts (BVerfG) vom 17.07.2013 dürfen Versicherungsunternehmen (VU) Ihre KundInnen nicht zu einer pauschalen Gesundheitsauskunft verpflichten (1 BvR 3167/08). Fehlt eine gesetzliche Regelung, so ist es zur Gewährleistung eines schonenden Ausgleichs der verschiedenen Grundrechtspositionen möglicherweise geboten, durch eine verfahrensrechtliche Lösung im Dialog zwischen Versichertem und Versicherer die zur Abwicklung des Versicherungsfalls erforderlichen Daten zu ermitteln. Die Anforderungen an diesen Dialog können Zivilgerichte festlegen.

Das BVerfG gab einer Frau Recht, die wegen einer Depression ihren Berufsunfähigkeitsversicherer (VU) in Anspruch nehmen wollte. Dieser verlangte von ihr weitreichende Schweigepflichtentbindungen. Nach deren Tarifbedingungen hatte die Versicherte bei der Beantragung von Versicherungsleistungen unter anderem behandelnde Ärzte, Krankenhäuser und sonstige Krankenanstalten sowie Pflegepersonen, andere Personenversicherer und Behörden zu ermächtigen, dem VU auf Verlangen Auskunft zu geben. Die Beschwerdeführerin lehnte es ab, die auf dem Antragsformular des VU abgedruckte Schweigepflichtentbindungserklärung, die zur Einholung sachdienlicher Auskünfte bei einem weiten Kreis von Stellen ermächtigt hätte, abzugeben und bot stattdessen an, Einzelermächtigungen für jedes Auskunftsersuchen zu erteilen. Daraufhin übersandte das VU der Beschwerdeführerin vorformulierte Erklärungen zur Schweigepflichtentbindung ihrer Krankenkasse, zweier Ärztinnen und ihrer Rentenversicherung, die die verschiedenen Stellen „umfassend" zur Auskunftserteilung über „Gesundheitsverhältnisse, Arbeitsunfähigkeitszeiten und Behandlungsdaten" sowie im Fall der Rentenversicherung über die „berufliche Situation" ermächtigen sollten. Die Beschwerdeführerin lehnte auch die Unterzeichnung dieser Erklärungen ab und bat um weitere Konkretisierung der gewünschten Auskünfte. Dem kam das VU nicht nach.

Die Klage der Beschwerdeführerin auf Zahlung der monatlichen Rente hatten die Zivilgerichte abgeweisen mit der Begründung, der Beschwerdeführerin sei zumutbar gewesen, die Einzelermächtigungen vor der Unterzeichnung selbst weiter einzuschränken oder die in den Einzelermächtigungen genannten Unterlagen selbst zu beschaffen und der Beklagten vorzulegen. Das BVerfG entschied nun, dass die gerichtlichen Entscheidungen die Beschwerdeführerin in ihrem durch Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG gewährleisteten allgemeinen Persönlichkeitsrecht in seiner Ausprägung als Recht der informationellen Selbstbestimmung verletzen.

Aus dem Recht auf informationelle Selbstbestimmung folge eine Schutzpflicht des Staates. Kann in einem Vertragsverhältnis ein Partner den Vertragsinhalt faktisch einseitig bestimmen, sei es Aufgabe des Rechts, auf die Wahrung der Grundrechtspositionen der beteiligten Parteien hinzuwirken. Zwar hat der Gesetzgeber inzwischen in § 213 VVG eine Regelung zum Schutz der informationellen Selbstbestimmung der Versicherungsnehmer getroffen; diese Vorschrift fand jedoch auf den zu entscheidenden Altfall noch keine Anwendung. Daher oblag es in diesem Fall den Gerichten, das Recht auf informationelle Selbstbestimmung durch einen angemessenen Ausgleich mit dem Offenbarungsinteresse des VU zu gewährleisten. Dabei sind die gegenläufigen Belange im Rahmen einer umfassenden Abwägung gegenüberzustellen. Das VU muss einerseits den Eintritt des Versicherungsfalls prüfen können; anderseits muss die Übermittlung von persönlichen Daten auf das hierfür Erforderliche begrenzt bleiben. Allerdings ist es dem VU oft nicht möglich, im Voraus alle Informationen zu beschreiben, auf die es für die Überprüfung des Leistungsfalls ankommen kann. Soweit keine gesetzlichen Regelungen zur informationellen Selbstbestimmung greifen, kann es zur Gewährleistung eines schonenden Ausgleichs der verschiedenen Grundrechtspositionen geboten sein, z. B. durch eine verfahrensrechtliche Lösung im Dialog zwischen Versichertem und VU die zur Abwicklung des Versicherungsfalls erforderlichen Daten zu ermitteln. Die Anforderungen an diesen Dialog festzulegen und ihn auszugestalten, zähle zu den Aufgaben der Zivilgerichte. Versicherte einer Berufsunfähigkeitsversicherung können nicht auf die Möglichkeit verwiesen werden, einen Vertragsschluss zu unterlassen oder die Leistungsfreiheit des Versicherers hinzunehmen.

Diesen verfassungsrechtlichen Anforderungen genügten die angegriffenen Zivilgerichts-Entscheidungen nicht, weil sie den Belangen der Beschwerdeführerin nicht hinreichend Rechnung trugen. Durch die vorformulierten Einzelermächtigungen würde dem VU ermöglicht, auch über das für die Abwicklung des Versicherungsfalls erforderliche Maß hinaus in weitem Umfang Informationen über die Beschwerdeführerin einzuholen. Die

benannten Gegenstände der „umfassenden“ Auskünfte – etwa „Gesundheitsverhältnisse, Arbeitsunfähigkeitszeiten und Behandlungsdaten“ – sind so allgemein gehalten, dass sie kaum zu einer Begrenzung des Auskunftsumfangs führen. Erfasst werden nahezu alle bei den benannten Auskunftsstellen über die Beschwerdeführerin vorliegenden Informationen, darunter auch viele für die Abwicklung des Versicherungsfalls bedeutungslose Informationen.

Das BVerfG entschied, der Beschwerdeführerin sei es nicht zuzumuten die vorformulierten Einzelermächtigungen selbst zu modifizieren oder die erforderlichen Unterlagen eigenständig vorzulegen. Denn damit würde der Beschwerdeführerin auferlegt, die Interessen des VU zu erforschen, und für den Fall, dass die vorgelegten Unterlagen oder die modifizierten Ermächtigungen für unzureichend erachtet würden, mit dem Risiko eines Leistungsverlusts belastet werden. Dieser Weg sei nicht geeignet, ihr Recht auf informationelle Selbstbestimmung im Dialog mit dem VU zu gewährleisten. Das beklagte VU werde nicht unverhältnismäßig belastet, wenn von ihm eine weitere Einschränkung der geforderten Einzelermächtigungen verlangt wird. Zwar könne der Umfang der Einzelermächtigungen dabei nicht vornherein schon auf die für die Prüfung des Leistungsanspruchs relevanten Informationen begrenzt werden. Wird die Schweigepflichtentbindung aber zunächst auf solche Vorinformationen beschränkt, die ausreichen, um festzustellen, welche Informationen tatsächlich für die Prüfung des Leistungsfalls relevant sind, könnte so der Umfang der überschießenden Informationen begrenzt und damit dem Recht der Beschwerdeführerin auf informationelle Selbstbestimmung Rechnung getragen werden. Die Verfahrenseffizienz würde durch eine solche grobe Konkretisierung der Auskunftsgegenstände nur geringfügig beeinträchtigt.

Der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) wies darauf hin, dass er bereits im September 2007 nach einer entsprechenden Entscheidung des BVerfGs empfohlen hatte, bei der Bearbeitung von Versicherungsfällen die neue Rechtslage zu berücksichtigen. Am 17.01.2012 bestätigte der Zusammenschluss der deutschen Datenschutzaufsichtsbehörden, der Düsseldorfer Kreis, nach langen Verhandlungen mit dem GDV dessen Formulierungsvorschläge für eine datenschutzkonforme Entbindung von der Schweigepflicht (BVerfG PM Nr. 53/2013 v. 13.08.2013; Gericht bremst Datenhunger, SZ 14./15.08.2013; B. DK v. 17.01.2013, http://www.datenschutz.hessen.de/dk20120117.htm#entry3741).

BGH

Zwang zu ungesicherter E-Mail-Kommunikation ist unzumutbar

Der Kartellsenat des Bundesgerichtshofs (BGH) hat am 26.02.2013 folgenden Beschluss gefasst (Az. KVZ 57/12): „Die Beschwerde der Landeskartellbehörde Brandenburg gegen die Nichtzulassung der Rechtsbeschwerde in dem Beschluss des Kartellsenats des Brandenburgischen Oberlandesgerichts vom 11. September 2012 wird zurückgewiesen. Die im Nichtzulassungsbeschwerdeverfahren angefallenen Kosten und Auslagen trägt die Landeskartellbehörde. Der Gegenstandswert der Nichtzulassungsbeschwerde wird auf 500 € festgesetzt.

Gründe: Die Nichtzulassungsbeschwerde ist zurückzuweisen, weil keiner der in § 74 Abs. 2 GWB vorgesehenen Gründe vorliegt, nach denen der Senat die Rechtsbeschwerde zulassen darf. Das Verfahren hat weder grundsätzliche Bedeutung, noch erfordert es eine Entscheidung des Rechtsbeschwerdegerichts zur Fortbildung des Rechts oder zur Sicherung einer einheitlichen Rechtsprechung.

Dabei kann offenbleiben, ob das Beschwerdegericht zu Recht angenommen hat, in der Excel-Datei, deren Übermittlung durch eine E-Mail die Landeskartellbehörde verlangt hat, seien Betriebs- und Geschäftsgeheimnisse enthalten gewesen (vgl. dazu BGH, Urteil vom 20.07.2010 - EnZR 24/09, NVwZ-RR 2011, 58 Rn. 35). Denn jedenfalls ist der Betroffene nicht verpflichtet, unternehmensinterne Daten über eine ungesicherte E-Mail-Verbindung an die Behörde zu übermitteln. Nach den Feststellungen des Beschwerdegerichts stellt die Landeskartellbehörde nur eine E-Mail-Adresse zur Verfügung, die lediglich zum Empfang nichtsignierter und nichtverschlüsselter Nachrichten dient. Auch soweit es sich bei den übermittelten Daten nicht um Betriebs- oder Geschäftsgeheimnisse handelt, ist es einem Unternehmen nicht zumutbar, einen derartigen Übertragungsweg benutzen zu müssen, zumal die Landeskartellbehörde die Möglichkeit hat, sich die gewünschte Datei auf anderem Wege, etwa auf einem Datenträger oder auf einem gesicherten elektronischen Übertragungsweg, übermitteln zu lassen.“

BGH

Bankauskunft bei Produktfälschung

Der Bundesgerichtshof (BGH) hat Beschluss vom 17.10.2013 entschieden, dass Markeninhaber einen Anspruch auf Bankauskunft haben, um über die Konten, die beim Vertrieb gefälschter Produkte angegeben werden, an die Namen von Produktfälschern heranzukommen (Az: I ZR 51/12). Weil es dafür auf europäisches Recht ankommt, hat der BGH den Fall dem Europäischen Gerichtshof (EuGH) vorgelegt. Der Online-Vertrieb von Produktfälschungen beschäftigt den BGH seit Jahren. Der Wettbewerbssenat versucht einerseits, den Markeninhabern die Instrumente an die Hand zu geben, um gegen die Fälscher vorzugehen. Im Frühjahr 2012 gewährte das Gericht ihnen beispielsweise eine erleichterte Beweislast, wenn es um den Nachweis von Fälschungen geht. Zugleich aber ist das Gericht bemüht, Geschäftsmodelle wie jenes der Online-Plattform Ebay nicht mit unerfüllbaren Prüfpflichten zu belasten.

Diese Linie wird mit dem Beschluss weiterverfolgt: Geklagt hatte die Coty Germany GmbH, die unter anderem Davidoff-Parfüms vertreibt. Das Unternehmen war im Januar 2011 auf ein bei eBay angebotenes gefälschtes Parfüm der Marke „Davidoff Hot

Water" aufmerksam geworden. Die Firma ersteigerte das Parfüm, kam aber bei der Suche nach den Hintermännern des illegalen Angebots nicht weiter, weil der vermeintliche Verkäufer die Auskunft verweigerte. Daraufhin ersuchte sie eine Sparkasse, ihr den Inhaber des angegebenen Kontos zu nennen. Diese verweigerte dies unter Hinweis auf das Bankgeheimnis. Dass die Bank dazu nach dem deutschen Markengesetz berechtigt war, steht außer Zweifel. Allerdings könnte sich, so jetzt der BGH, aus der EU-Richtlinie zur Durchsetzung der Rechte des geistigen Eigentums darüber hinausgehend ein Auskunftsanspruch ergeben. Das Interesse an einer effektiven Verfolgung von Markenrechtsverletzungen müsse Vorrang haben vor dem Interesse der Bank, die Identität des Kontoinhabers geheim zu halten. Senatsvorsitzender Joachim Bornkamm: „Sonst wäre es allzu leicht, unter Verdeckung der Identität Rechtsverletzungen zu begehen." Die Abwägung müsse zugunsten des Unternehmens ausfallen, weil die Identität eines Kontoinhabers, der mithilfe dieser Bankverbindung Geschäfte betreibe, „keine besonders sensible Information" sei. Weil die Rechtslage nach EU-Recht aber nicht eindeutig ist, legte der BGH den Fall dem EuGH als obersten EU-Gericht zur Entscheidung vor (Janisch, Drei, zwei, eins, Auskunft, http://www.sueddeutsche.de 18.10.2013, SZ 18.10.2013, 23).

BAG

Arbeitnehmer zur elektronischen Signatur verpflichtet

Das Bundesarbeitsgericht (BAG) hat mit Urteil vom 25.09.2013 entschieden, dass ein Arbeitgeber von seiner ArbeitnehmerIn die Beantragung einer qualifizierten elektronischen Signatur und die Nutzung einer elektronischen Signaturkarte verlangen kann, wenn dies für die Erbringung der Arbeitsleistung erforderlich und dem Arbeitnehmer zumutbar ist. Eine Verwaltungsangestellte im Wasser- und Schifffahrtsamt Cuxhaven, zu deren Aufgaben die Veröffentlichung von Ausschreibungen bei Vergabeverfahren gehört, hatte geklagt. Seit dem 01.01.2010 erfolgen diese Veröffentlichungen nur noch in elektronischer Form auf der Vergabeplattform des Bundes. Zur Nutzung wird eine qualifizierte elektronische Signatur benötigt, die nach den Bestimmungen des Signaturgesetzes (SigG) nur natürlichen Personen erteilt wird. Die Behörde wies die Klägerin an, eine solche Signatur bei einer vom SigG vorgesehenen Zertifizierungsstelle, einem Tochterunternehmen der Deutschen Telekom AG, zu beantragen. Dazu müssen die im Personalausweis enthaltenen Daten zur Identitätsfeststellung an die Zertifizierungsstelle übermittelt werden. Die Kosten für die Beantragung trägt die Arbeitgeberin.

Die Klägerin hatte die Auffassung vertreten, der Arbeitgeber könne sie nicht verpflichten, ihre persönlichen Daten an Dritte zu übermitteln. Auch sei nicht sichergestellt, dass mit ihren Daten kein Missbrauch getrieben werde. Nachdem das Arbeitsgericht und das Landesarbeitsgericht die Klage abgewiesen hatte, blieb die Klägerin mit ihrer Revision auch vor dem BAG erfolglos. Die Beklagte habe von ihrem arbeitsvertraglichen Weisungsrecht (§ 106 GewO) angemessen Gebrauch gemacht. Der mit der Verpflichtung zur Nutzung einer elektronischen Signaturkarte verbundene Eingriff in das Recht auf informationelle Selbstbestimmung sei der Klägerin zumutbar. Die Übermittlung der Personalausweisdaten betreffe nur den äußeren Bereich der Privatsphäre; besonders sensible Daten seien nicht betroffen. Der Schutz dieser Daten werde durch die Vorschriften des SigG sichergestellt; sie würden nur durch die Zertifizierungsstelle genutzt. Auch durch den Einsatz der Signaturkarte entstünden für die Klägerin keine besonderen Risiken. So enthalte die mit dem Personalrat abgeschlossene Dienstvereinbarung ausdrücklich eine Haftungsfreistellung; die gewonnenen Daten dürften nicht zur Leistungs- und Verhaltenskontrolle durch den Arbeitgeber verwendet werden (Verpflichtung zur Nutzung einer elektronischen Signaturkarte, juris.bundesarbeitsgericht.de, BAG PM Nr. 56/13).

LG Mönchengladbach

Kein Ausschluss von der Suche bei Persönlichkeitsverletzung

Das Landgericht (LG) Mönchengladbach wies am 05.09.2013 die Klage eines Professors ab, mit der dieser Google untersagen wollte, Persönlichkeitsrechtsverletzungen gegen sich in den Suchergebnissen anzeigen. Der Politikwissenschaftler aus Düsseldorf wird auf einer anonym betriebenen Seite im Internet als „Linksextremist" und „Teil des bundesdeutschen Stasi-Netzwerks" bezeichnet. Der Professor im Ruhestand war 2010 in der Lehrerweiterbildung gegen Neonazis aktiv, worüber sich der rechte Blogbetreiber empörte. Ihm ging es weniger darum, die eigentliche Beleidigung aus dem Netz zu löschen, als zu verhindern, dass jemand die bösartige Kritik finden kann. Wer bei Google nur nach dem Namen des Wissenschaftlers sucht, findet den beleidigenden Text direkt an erster oder zweiter Stelle in den Suchergebnissen. Das ist aus Perspektive des Klägers unangenehm. Jeder, der sich für seine Person interessiert und über die Suchmaschine recherchiert, stößt zunächst auf die Beleidigung. Würde Google die Seite aus dem Index der durchsuchbaren Seiten nehmen, könnten Nutzer den Text nicht mehr finden. In einem solchen Fall wäre dies fast gleichbedeutend mit einer Löschung des ganzen Textes.

Die Richter teilten jedoch die Auffassung von Google, wonach der Konzern seine Suchergebnisse inhaltlich nicht zu bewerten oder zu verändern habe. Die Suche zeige lediglich, was sich im Netz finden lasse, dieser Vorgang sei „mathematisch". Das Gericht warf dem Kläger außerdem vor, sich nicht genügend um die Löschung des Textes gekümmert zu haben. Er hätte seine Energie weniger auf Google, denn auf Wordpress konzentrieren sollen. Der amerikanische Anbieter betreibt das Blog-Angebot, auf dem der beleidigende Text eingestellt wurde. Der Wissenschaftler konnte den Urheber nicht ausfindig machen; Wordpress hatte auf seine Beschwerde nicht reagiert.

Es gibt eine Menge Hetz- und Hassseiten im Netz, auf denen Menschen beleidigt werden. Viele von ihnen werden so geschickt anonym betrieben, dass eine Löschung oder Ermittlungen unmöglich sind. Google erschließt auch diese Seiten. Mit den Suchergebnissen, die der Konzern bei der Suche nach einer Person ausgibt, formt er maßgeblich das Bild, das sich Netznutzer von diesem Menschen machen. Der Kläger kann in Berufung gehen (Boie, Ein Treffer beleidigt, SZ 06.09.2013, 29; Sawall, Google-Suche muss rechtes Schmähblog nicht ausblenden, www.golem.de 06.09.2013; Google muss Suchergebnis nicht entfernen, www.heise.de 05.09.2013).

VG Aachen

Herausgabe von Telefonverzeichnis nach IFG

Das Verwaltungsgericht (VG) Aachen hat mit Urteil vom 17.07.2013 entschieden, dass ein Rechtsanwalt unter Berufung auf das Informationsfreiheitsgesetz (IFG) des Landes Nordrhein-Westfalen Anspruch auf Aushändigung des Telefonverzeichnisses des Verwaltungsgerichts hat (Az.: 8 K 532/11). Die Gerichtsleitung war dem Begehren des Anwalts mit dem Argument entgegen getreten, die dienstlichen Durchwahlnummern seien personenbezogene Daten, deren Weitergabe nur mit Einwilligungen der betroffenen Beschäftigten zulässig wäre, die aber nicht erteilt worden seien. Das Urteil ist nicht rechtskräftig (VG: Aachen: Gerichtsleitung muss Rechtsanwalt Telefonverzeichnis des Gerichts zur Verfügung stellen, beck-aktuell.beck.de 25.10.2013).

VG Schleswig

Fanpagebetreiber für mögliche Datenschutzverstöße nicht verantwortlich

Das Schleswig-Holsteinische Verwaltungsgericht (VG) hat auf drei Klagen von Unternehmen in Schleswig-Holstein – u. a. der Wirtschaftsakademie der Industrie- und Handelskammer (IHK) – am 09.10.2013 geurteilt, dass deutsche Betreiber von Facebook-Fanpages für die bei Facebook erfolgende Datenverarbeitung datenschutzrechtlich in keiner Weise verantwortlich gemacht werden können (Az. 8 A 37/12, 8 A 14/12, 8 A 218/11). Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) hatte Ende 2011 festgestellt, dass die Facebook-Datenverarbeitung nicht mit deutschem Datenschutzrecht vereinbar sei, u. a. weil die Nutzung von Fanpages personenbezogen präzise erfasst wird, gegen die Profilbildung keine Widerspruchsmöglichkeit eingeräumt wird, beim Setzen von Cookies keine wirksamen Einwilligungen eingeholt werden und weil für die Betroffenen nicht die geforderte Transparenz hergestellt wird. Das ULD hatte daraufhin den drei Unternehmen Ende 2011 per Verfügung auferlegt, ihre Fanseiten zu deaktivieren. Diese Bescheide wurden nun aufgehoben.

In der mündlichen Urteilsbegründung erklärte der Vorsitzende Richter, Fanpagebetreiber könnten für den von ihnen genutzten Dienst datenschutzrechtlich nicht verantwortlich gemacht werden, weil sie direkt auf das Angebot von Facebook keinen Einfluss nehmen können und auch keinen Zugriff auf die personenbezogenen Daten hätten. Facebook stelle die technische Infrastruktur zur Verfügung. Die Seiteninhaber könnten lediglich ihre Inhalte einstellen, hätten aber auf den Datenverkehr zwischen den Nutzenden und Facebook keinen Einfluss. Dass dies faktisch zu einer Beschränkung des Datenschutzes führe, müsse angesichts der gesetzlichen Regelung hingenommen werden. Das Gericht ließ offen, ob und in welchem Umfang die Erfassung von Daten der Nutzenden von Fanpages gegen das Datenschutzrecht verstoßen. Wegen der grundsätzlichen Bedeutung der Urteile ließ das VG die Berufung zu. In Entscheidungen Anfang des Jahres hatten das VG wie auch das Oberverwaltungsgericht entschieden, dass auch Facebook in Irland bzw. USA selbst nicht zur Anwendung des deutschen Datenschutzrechtes verpflichtet werden kann (DANA 1/2013, 41).

Marcus Schween, Federführer Recht der IHK Schleswig-Holstein freute sich: „Auch schleswig-holsteinische Unternehmen können, wie alle anderen Unternehmen in Deutschland und Europa, soziale Netzwerke wie Facebook als Kommunikations- und Vertriebskanal nutzen. Für die IHK war es ein wichtiges Ziel Rechtssicherheit herzustellen.“ Die Aktion der Landesdatenschützer sei geeignet gewesen, eine erhebliche Wettbewerbsverzerrung für Unternehmen in Schleswig-Holstein zu bewirken. Thilo Weichert, Leiter des ULD, zeigte sich dagegen enttäuscht: „Für den Datenschutz im Internet sind die Entscheidungen eine weitgehende Kapitulation: Angesichts der üblichen Arbeitsteilung können sich Anbieter damit herausreden, sie hätten keinen Einfluss auf die von ihnen eingesetzten, im Ausland betriebenen Programme. Der Gedanke des Grundrechtsschutzes spielte, so zumindest unser Eindruck, keine wesentliche Rolle. Wir meinen, dass die Anbieter durch die Auswahl ihrer Dienstleister für deren Datenschutzverstöße zumindest mit verantwortlich sind. Wir werden die schriftlichen Gründe des Gerichts genau prüfen und voraussichtlich eine Entscheidung durch das Oberverwaltungsgericht anstreben“ (Verwaltungsgericht hebt Anordnungen des ULD betreffend Fanpages bei Facebook auf, PE OVG Schleswig-Holstein 09.10.2013; Verwaltungsgericht: Fanpage-Betreiber unverantwortlich für Facebook-Datenverarbeitung, PM ULD 09.10.2013).

Buchbesprechung



Däubler, Wolfgang
Internet und Arbeitsrecht
Bund Verlag Frankfurt a. M., 4. Aufl. 2013, 421 S., ISBN 978-3-7663-6227-8

(tw) Der Autor Wolfgang Däubler gehört zu den ArbeitsrechtlerInnen, die sich über Jahrzehnte hinweg den Ruf besonderer Expertise und zugleich des Engagements für die Interessen der ArbeitnehmerInnen erarbeitet und bewahrt haben. Er gehört zudem zu den Pionieren des Technik- und Datenschutzrechts im Bereich der Beschäftigtenverhältnisse, was er u. a. als Coautor eines Kommentars zum Bundesdatenschutzgesetz (Däubler/ Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, 4. Aufl. 2013) sowie als Autor der „Gläsernen Belegschaften“ (6. Aufl. erscheint auch im Herbst 2013) unter Beweis stellt. Der Umstand, dass das 2001 erstmals aufgelegte Thema „Internet und Arbeitsrecht“ schon in der 4. Auflage erscheint, zeigt, dass diese Materie einer sehr schnellen technischen wie rechtlichen Entwicklung unterworfen ist, die der Autor durch umfassende Berücksichtigung der praktischen Entwicklungen sowie der Dogmatik in Rechtsprechung und Lehre berücksichtigt: Stichworte sind Social Media, E-Mail-Nutzung oder Bring your own Device (BYOD).

Interessant sind für die DatenschützerIn nicht nur die klassischen Themen der Beschäftigtenkontrolle über das Netz, der privaten und dienstlichen Nutzung oder der Abgrenzung zwischen Persönlichkeitsschutz und Meinungsfreiheit, sondern auch die Fragen des Mitbestimmungsrechts, der Internetnutzung durch den Betriebsrat, der Pflichtverstöße von ArbeitnehmerInnen im Zusammenhang mit dem Netz oder Web-Arbeitsverhältnisse. Am Ende des Werks werden Formulierungsvorschläge für Betriebsvereinbarungen gemacht und nützliche Informationen gegeben für weitere Recherchen und Aktivitäten. Das Buch erfüllt alle Erwartungen an ein Handbuch: gut recherchiert, umfassend, informativ, für Laien verständlich, ausgiebige Quellenangaben, gut strukturiert und erschlossen – und das insbesondere auch für DatenschützerInnen, die mit Arbeitsverhältnissen und dem Internet zu tun haben.



Rupp, Martin
Die grundrechtliche Schutzpflicht des Staates für das Recht auf informationelle Selbstbestimmung im Pressesektor
Verlag Alma Mater, Saarbrücken, 2013, ISBN 978-3-935009-55-3, 352 S.

(tw) Es gibt inzwischen viele Dissertationen zum Thema Datenschutz; nicht alle bedürfen der öffentlichen Aufmerksamkeit und der Besprechung. Bei der von Prof. Christoph Gröpl betreuten Promotionsschrift ist Kenntnisnahme und Diskussion angeraten, da sich der Autor Fragen widmet, die noch nicht in Rechtsprechung, Literatur und Praxis ausdiskutiert sind: Es geht um die grundlegende Frage der staatlichen Schutzpflicht in Sachen Datenschutz und dann um die Frage des Verhältnisses des Datenschutzes zur Pressefreiheit. Rupp behandelt auf diesen Grunderwägungen die Frage, inwieweit die presserechtlichen Landesregelungen zum Datenschutz ausreichend sind und kommt zu dem Ergebnis „Nein“. Tatsächlich trauen sich bisher weder der Gesetzgeber noch die Datenschutzaufsichtsbehörden so richtig an die Klärung der Grenzen zwischen informationeller Selbstbestimmung und Pressefreiheit. Angesichts der Relevanz dieses Grenz-, Konflikt- und Ergänzungsverhältnisses, insbesondere im Hinblick auf die Nutzung des Internets durch die Presse, ist diese Abstinenz nicht zu rechtfertigen.

Interessant ist schon der Ausgangspunkt von Rupps Überlegungen: Bevor er sich dem Widerstreit der Grundrechte auf Datenschutz und auf Pressefreiheit widmet, befasst er sich mit den Grundlagen staatlicher Schutzpflichten für die Grundrechte. In Fortentwicklung der bisherigen Rechtsprechung kommt er dabei zu dem Ergebnis, dass diese Schutzpflicht, die Legislative, Exekutive und Judikative bindet, auch im Hinblick auf das Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG gilt. Dabei prüft der Autor vorrangig den legislativen Gestaltungsspielraum. Angesichts der massiven Vollzugsdefizite insbesondere beim Internetdatenschutz wäre auch die Frage spanend, welche Handlungs- und Auslegungspflichten sich für die Datenschutzaufsicht und die Rechtsprechung ergeben. Hinsichtlich der Legislative prüft Rupp auf drei Stufen, die er „Evidenzkontrolle“, „Vertretbarkeitskontrolle“ und „intensivierte inhaltliche Kontrolle“ nennt.

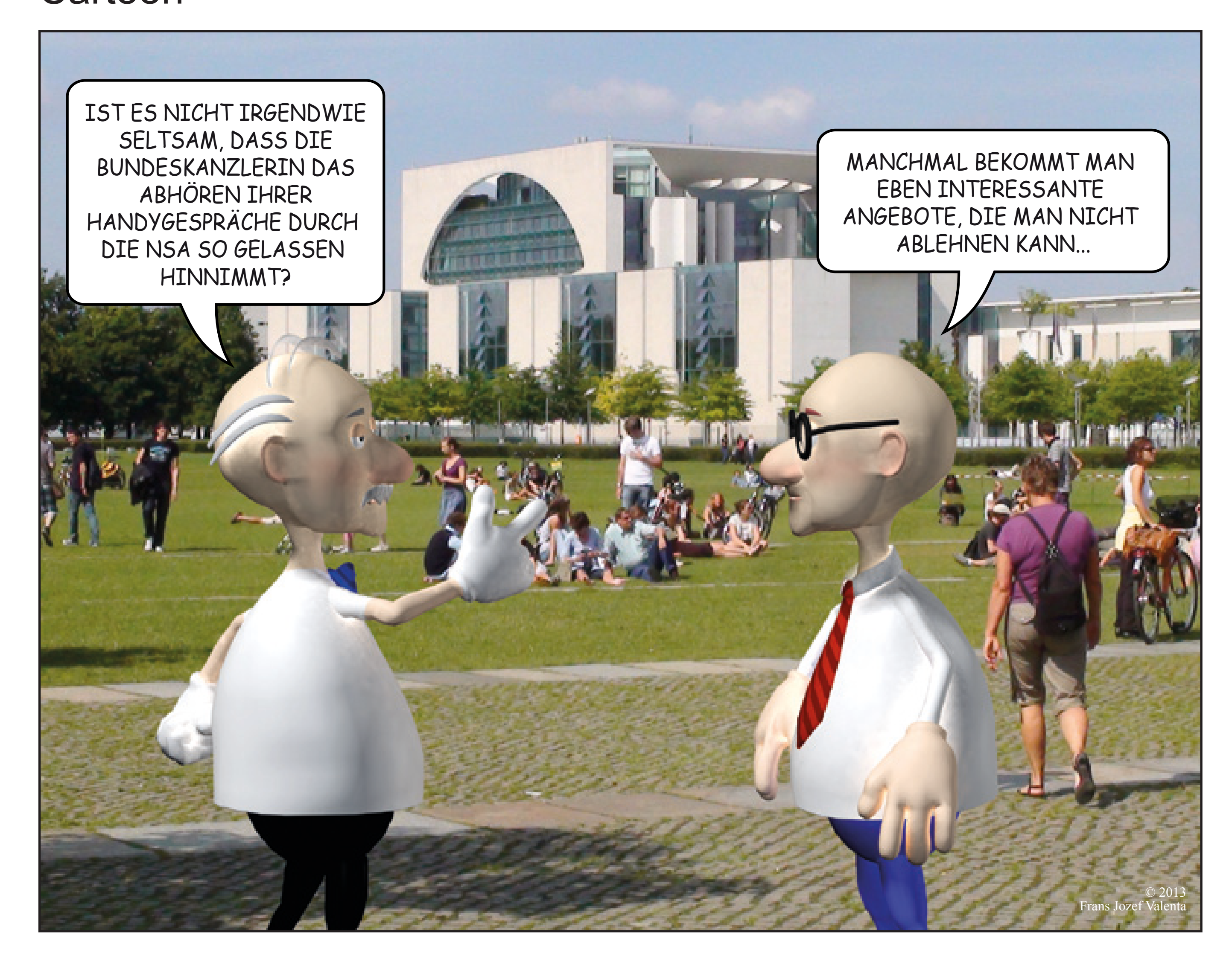
Bei Anwendung dieses Prüfungsmaßstabes kommt Rupp zu dem Ergebnis, dass die Privilegierungen der Presse gemäß § 41 Abs. 1 BDSG i. V. m.

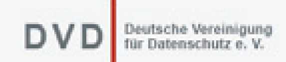
Landespresserecht zu weit gehen, indem sie den Redaktionsdatenschutz der Selbstregulierung des Deutschen Presserates überlassen: Die Teilnahme hieran ist freiwillig; rechtsverbindliche Verfahren und Sanktionen bestehen nicht; es wird eine monistische, also einseitig presselastige Aufsicht praktiziert; wirksame präventive Instrumente fehlen. Dadurch werde der verfassungsrechtlich geforderte Regelungsrahmen unterschritten.

Rupp schlägt in Konsequenz vor, die gesetzlichen Regelungen auszubauen und dadurch den selbstregulatorischen Ansatz mit einer höheren Legitimation und Verbindlichkeit zu versehen. Dies könne zunächst darin bestehen, dass der Pressekodex gemäß § 38a BDSG hoheitlich überprüft und autorisiert wird. Nötig seien außerdem eine gesetzlich verbindlichere Rügenveröffentlichungspflicht und eine Pluralisierung des Beschwerdeausschusses. Über eine Rückfallklausel solle sichergestellt werden, dass sich Presseunternehmen durch Kündigung der Selbstverpflichtung nicht jeder Kontrolle entziehen, sondern dann verstärkten Auskunfts-, Verfahrens- und Haftungspflichten unterworfen werden.

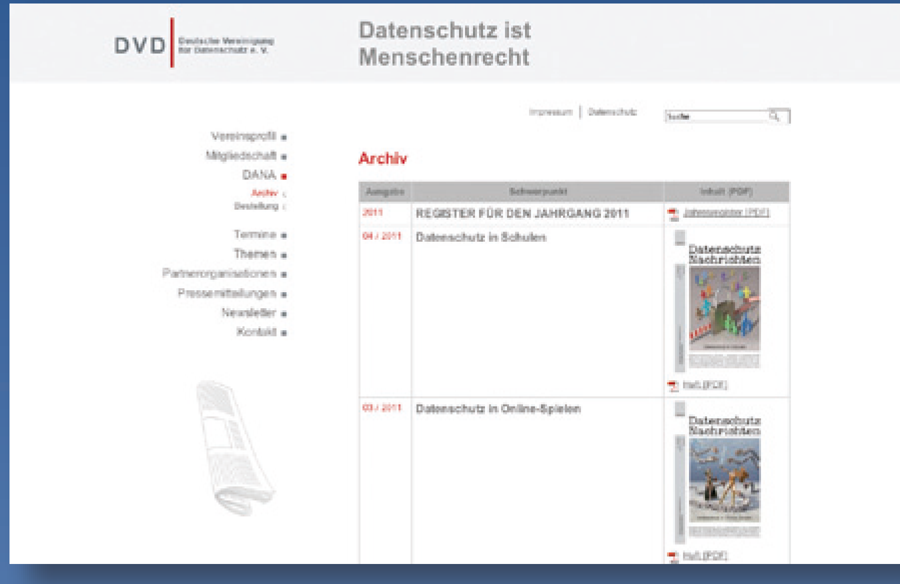
Der Autor stellt schlicht fest, dass sich derzeit das Presserecht nicht auf der grundrechtlichen Höhe des nötigen Datenschutzes befindet und fordert von den Landesgesetzgebern ein Tätigwerden. Er belässt es nicht beim Appell, sondern macht konkrete Formulierungsvorschläge. Nicht nur diese sind valide, sondern die gesamte Arbeit. Zwar nähert sich der Autor auf klassische Doktorandenweise tastend seinem Thema, indem er bei altbekannten Basics startet. Doch bleibt er nicht dort stehen, sondern entwickelt konsequent seine Sicht bis hin zu den rechtspolitischen Forderungen. Dabei befasst er sich umfassend mit dem Spannungsverhältnis von Pressefreiheit und Datenschutz und erschließt im Anhang hierzu viele brauchbare Fakten: Literatur, alle entscheidenden Gesetze, relevante Gerichtsentscheidungen bis hinein in die Gegenwart, Satzung, Geschäftsordnung, Beschwerdeordnung und Kodex des Deutschen Presserates. Das Ganze ist zudem verständlich formuliert, gut gegliedert und somit auch inhaltlich leicht erschließbar, so dass diese Promotion als Handbuch für das allgemeine Pressedatenschutzrecht zweckentfremdet genutzt werden kann.

Cartoon











Die neue DVD-Webseite

Sie war ein wenig in die Jahre gekommen, unsere Website. Und weder die aktuelle DANA noch die alten Hefte wurden angemessen präsentiert. Der Vorstand hatte daher schon vor einiger Zeit eine Erneuerung beschlossen. Bei dieser Gelegenheit sollten auch alte Zöpfe abgeschnitten werden, wie z. B. die Schwarze Liste, die bei heutigen technischen Möglichkeiten nicht mehr sinnvoll schien. Der optische Eindruck hingegen sollte möglichst erhalten bleiben.

Auch wenn sich einige Bereiche noch in Arbeit befinden, haben wir uns bereits jetzt für eine Veröffentlichung entschieden. Denn es ist auf Dauer zu aufwändig, zwei Webauftritte parallel zu pflegen.

Die wichtigsten Neuerungen:

- Die DANA wird jetzt heftweise präsentiert. Zwei Jahren lang ist neben dem Titelbild der Ausgabe auch das Inhaltsverzeichnis abrufbar. Nach Ablauf dieser Zeit wandert das Heft in den Archivbereich und ist dann kostenlos als PDF erhältlich.
- Anmeldungen zu Presseverteiler und Mitgliederverteiler werden nun mittels double-opt-in-Verfahren umgesetzt.
- Der gesamte Webauftritt wird mittels SSL-Verschlüsselung übertragen, so dass auch Formulardaten wie Bestellungen oder Beitrittserklärungen verschlüsselt übertragen werden.
- Umstellung auf ein CMS, das uns die alltägliche Pflege sehr erleichtert. Das macht sich unter anderem bei der Aktualität der Termine bemerkbar.

Wir freuen uns über jede Anregung zur Füllung der Themenseiten oder über Hinweise auf datenschutzbezogene, nichtkommerzielle Veranstaltungen.